OnGo Roaming Whitepaper

September 2023

Executive Summary

Table of Contents

Table of Figures

Table of Tables

1 Executive Summary

The Roaming Whitepaper focuses on identification of the key issues and challenges for using a Citizens Broadband Radio Service (CBRS) Shared Home Network Identifier (SHNI) Subscriber Identity Module (SIM) with the common roaming architecture models of Home Routed (HR), Roaming Hub and Local Breakout (LBO). The purpose of this paper is to evaluate these architecture models in contrast to a Dual-SIM solution. There are no recommendations or conclusions derived within this paper, but as a general summary, there is no single roaming architecture model that is without problems to solve.

The approach to the paper is to evaluate each roaming architecture model against the end user roaming directions of Private-to-Public, Public-to-Private, and Private-to-Private. An important foundation of this paper is to provide background information on the roaming environment, including the role of GSMA, the 3GPP standard architecture models, the interconnection methods, background on CBRS, and general information on wholesale billing and settlement. While there are some inclusions of 5G SA roaming within this paper, the primary focus is on 4G LTE.

The number of documented issues related to the Private-to-Public roaming direction in a descending order are LBO, Roaming Hub, and HR. While the HR model has the lowest numerical count of key issues, the majority of these issues would need attention every time a new public MNO was connected to the Private Mobile Network Operator (MNO).

The number of documented issues related to the Public-to-Private roaming direction is low, however the most important well-known barrier to this roaming direction is device capabilities that include the CBRS band as well as operator preference, e.g., preferring a non-home Public Land Mobile Network (PLMN) over a home PLMN. These device specific aspects are out of scope of this whitepaper, but will need a solution before this roaming direction can be realized.

There is some general information included in this paper related to Multi-Operator Core Network (MOCN), specifically in contrast to a traditional inbound roaming (Public-to-Private) model. Further discussion on MOCN will be addressed in a different paper.

In addition, a Private-to-Private roaming direction is introduced with a novel Collaborative Camping model which does not align to the standard roaming models. This architecture model should be considered as highly customized for two or more dis-contiguous private networks that are collaborating to share network functions. However, there are multiple issues that would require a solution, most notably, a hierarchical Home Subscriber Server (HSS) structure.

Comparing all the documented issues for each roaming direction and architecture model, Internet Protocol Multimedia Subsystem (IMS) services represent the biggest problem area to solve. However, if IMS is not required for a private network, then these issues are mitigated by default. The next category is Domain Name Server (DNS) for Access Point Name (APN) resolution, followed by Diameter routing functions and local Mobility Management Entity (MME) configuration. There are also a significant amount of general architecture and interconnection issues that impact every roaming model in each roaming direction.

2 Introduction and Scope

The purpose of this whitepaper is to focus on methods for enabling roaming for OnGo Shared Home Network Identifier (SHNI) using a single Subscriber Identity Module (SIM) with a single International Mobile Subscriber Identity (IMSI) in multiple directions, and to identify key challenges that result from using a SHNI when interfacing with a commercial or private mobile network. Primarily, this paper focuses on the roaming directions of 1) Private-to-Public, 2) Public-to-Private, and 3) Private-to-Private where a private network refers to any entity that deploys and operates their own Radio Access Network (RAN) and Core using a Mobile Country Code (MCC) and Mobile Network Code (MNC) that is shared among other private entities in the 7th to 15th digit range. A public network refers to any commercially available Mobile Network Operator (MNO) using a dedicated MCC/MNC.

This paper will primarily focus on the Long-Term Evolution (LTE) RAN and Evolved Packet Code (EPC) as well as will briefly introduce some aspects related to a Next Generation (NG) RAN and 5th Generation (5G) Core (5GC). Multiple different roaming model options are presented for completeness; however, this paper is not intended to be a deployment guide or recommend any single option as a best practice. A historical review of standard roaming models and interconnection options are included to set a foundation for how private networks can interact with commercial MNO networks. The intention of this paper is for readers to focus on the specific architecture model(s) of interest with foundational review as needed.

This paper will also consider high level aspects related to rating and charging models, Service Level Assurance/Agreements (SLA) and generally discuss roaming agreements. It shall be noted that agreements with public or private MNO entities are highly customizable and therefore this information is included for reference only. Aspects related to dual SIM, emergency services, security, public safety, critical communications, and Multi-Operator Core Network (MOCN) are considered as out of scope for this paper.

3 Role of GSMA and 3GPP

The GSM Association (GSMA) and 3rd Generation Partnership Project (3GPP), among other standardization bodies, play a critical role in the success of telecommunications. For commercial MNOs, equipment suppliers, device manufacturers, and many others, both entities are crucial to ensuring a global network of interconnected MNOs are following the same set of guidelines. This section intends to provide foundational background for both GSMA and 3GPP for readers that may be unfamiliar with each entity's role in telecommunications services.

The GSMA is a consortium of more than 750 mobile operators as well as more than 400 companies worldwide that focuses on the development of the mobile ecosystem [1]. The GSMA has roots in Europe beginning in 1982 when the Confederation of European Posts and Telecommunications (CEPT) formed the Groupe Speciale Mobile with the mandate of designing a pan-European mobile technology [2]. Currently, in the mobile wireless world, mobile services were in the infancy stage with only analog-based technology available, and certainly not in mainstream usage. While there have been competing technologies over the years, such as Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), Integrated Digital Enhanced Network (iDEN), among others, Global System for Mobile Communications (GSM) based technologies prevailed and became the popular global standard. The work efforts throughout the 1980s paved the way for GSM based technology to be standardized and transformed into what we currently see as a global wireless network with interconnection capabilities.

Organizations cannot grow to the magnitude of GSMA without significant commitments from the business community. For the GSMA, this entails a membership structure that allows large and small businesses from all aspects of the telecommunications industry to join at the level that best suits the business. There are four primary membership types within GSMA: Operator, Industry, Rapporteur, and Sector [3]. According to GSMA [3], licensed mobile network operators are available to join as Operator members, if they are using a GSM family technology, such as GSM, 3G Universal Mobile Telecommunications System (UMTS) and/or Wideband Code Division Multiple Access (WCDMA), High Speed Packet Access (HSPA), LTE, or LTE-Advanced, while companies such as device manufacturers, software companies, equipment providers or internet providers are organizations, or providers of network software and equipment can join as Industry members. Rapporteur membership is available for "non-GSM licensed operators moving to LTE/HSPA, or those planning to roam on GSM networks – plus Mobile Virtual Network Operators" [3]. Finally, Sector membership is open to a wide range of potential businesses, covering, financial services, automotive, gaming, manufacturing, and many others [3].

The GSMA is involved in multiple different aspects of advancing mobile telecommunications and creating a better future. While no single organization can claim the vast achievements in mobile industry growth, it is arguable that GSMA has been one of the most influential. GSMA enables operators and vendor companies to work closely together to drive the needs of each respective business towards a brighter future, before and during, generational advancements. The smooth interconnection of mobile operators that enables a global mobile ecosystem is potentially one of the greatest achievements of GSMA.

The 3GPP is a multifaceted consortium of organizational partners encompassing seven telecommunication standards bodies with a focus on evolution of telecommunications systems [4]:

- **ARIB:** Association of Radio Industries and Businesses (Japan)
- **ATIS:** Alliance for Telecommunications Industry Solutions (United States of America)
- **CCSA:** China Communications Standards Association

- **ETSI:** European Telecommunications Standards Institute
- **TSDSI**: Telecommunications Standards Development Society India
- **TTA:** Telecommunications Technology Association (Republic of Korea)
- **TTC:** Telecommunication Technology Committee (Japan)

The original scope of 3GPP was to develop the standards that defined the creation of a 3G Mobile system evolved from a GSM based architecture and has since evolved to encompass systems beyond 3G [4]. 3GPP comprises three Technical Specification Groups (TSG), focusing on RAN, Services & Systems Aspects, and Core Network & Terminals (CT) and is contribution driven by member companies at a Working Group level [4]. The 3GPP has an intent focus on backwards compatibility to ensure uninterrupted service capability but is also a forward-looking organization and begins developing standards for new generational releases well in advance of commercial adoption [4].

Membership within 3GPP comprises Full, Individual, and limited duration Guest membership levels whereas each of the seven standards organizational bodies are Full members and a business entity that is a member of one of those organizations can become a Guest and eventually an Individual member [5]. Individual members typically comprise mobile network operators, network equipment and device suppliers and multiple other relevant businesses; a full list of members can be queried through 3GPP directly [6]. It should be noted that while a Guest member can be represented at group meetings, they cannot take part in “decision making, participate in discussions, contribute documents, or hold any leadership positions” [5].

3.1 GSMA Documents

The GSMA publishes multiple different types of documents for use within the telecommunications industry. Many of the documents take the form of reference material only, such as a Permanent Reference Document (PRD), and are non-binding. Most documents published by GSMA fit within a non-binding category, but some documents historically had been binding. An example of a binding document is BA.46 entitled Non-Terrestrial Roaming Principles, which defines the principles for operators that “provide coverage in International Zones and National Zones where they are authorized to do so” [7]. Another example is the IR.21 [8] entitled GSM Association Roaming Database, Structure and Updating Procedures, which provides the platform for roaming partners to exchange data relevant to the configuration of interconnection such as IP ranges, and International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) numbering schemes for E.164, E.212, and E.214 and other pertinent configuration details. The working groups within GSMA also drive the scope and context of the documents.

3.1.1 IR.21

The GSMA IR.21 [8] is the key document used for commercial MNOs and interconnection providers to exchange network configuration and identification data for the purpose of enabling unilateral or bilateral roaming. The IR.21 is a permanent reference document that is considered as Confidential and available to Operator, Rapporteur, Industry, and Sector GSMA members only, as such [8] refers to an older document version that is publicly accessible as a point of reference only. The format of the document follows a template that is created within the GSMA and recently has been integrated into the Roaming Agreement Exchange (RAEX) database with a defined schema for importing and exporting by member MNOs.

The relevance of the IR.21 for private wireless entities is to understand the types of network information exchanged between MNOs in the IR.21 to facilitate interconnection and roaming. There are some sections of the IR.21 that would not be relevant for a private network that is built based on 4G or above and relate directly

to Signaling System Number 7 (SS7) routing as well as alignment for ITU E.164 ranges, e.214 and a dedicated e.212. However, many other sections have significant relevancy in a 4G LTE interconnection, such as the Roaming and IP Interworking and LTE Roaming sections which are numbered as sections 17 and 20 of IR.21 respectively.

The Roaming and IP Interworking section includes the list of IP backbone ranges (IPv4 and/or IPv6) used for interconnection, the specific Domain Name System (DNS) addresses use for local caching and/or authoritative answers, as well as the unique Autonomous System Number (ASN) for the authoring MNO. Additionally, the LTE Roaming section includes the unique EPC Realm and information related to the interconnected Internet Protocol (IP) eXchange (IPX) provider for Diameter services. The relevance and importance of the IP information and LTE Roaming sections will be further described in section 4 covering interconnection with an IPX or MNO directly as well as in later sections discussing the roaming models and call flows for Diameter, Access Point Name (APN) resolution as well as data session establishment.

Additional sections are relevant to MNOs as needed, such as for Voice over LTE (VoLTE) Roaming, Roaming Hubs and for many other unique network details outside the scope of this paper.

3.1.2 IR.88

The GSMA IR.88 [9], current release v25.0, is a non-binding permanent reference document covering the Evolved Packet System (EPS) Roaming Guidelines. The IR.88 [9] covers architecture models specific to roaming when both visited and home public mobile networks (VPMN and HPMN) are EPS capable as well as for legacy interworking with 2G/3G systems using a S4 interface capable Serving General Packet Radio Service (GPRS) Support Node (SGSN). The relevant guidelines from IR.88 [9] that apply towards a private network entity interconnecting with a public MNO will be incorporated through this paper depending on the deployment model.

3.1.3 NG.113

The GSMA NG.113 [10], current release 4.0, is a non-binding permanent reference document covering the 5G System (5GS) Roaming Guidelines. The document is similar in scope and context to IR.88 [9] but focuses specifically on the 5GS and how roaming can function, as well as how interworking between a 5GS and EPC can occur based on home and serving network capabilities as well as roaming agreements.

3.2 3GPP Technical Specifications

There are numerous 3GPP technical specifications that outline the functionalities of all telecommunications system aspects for both the LTE EPC and the 5GS. For the purpose of this paper, included below in Table 1 is a short list of technical specifications that are useful for reference when interworking with a public MNO. The complete list of 3GPP specifications is available and accessible in [11].

Table 1: Key 3GPP Documents Addressing Roaming

Document	Title
23.401	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
24.301	Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
29.272	Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol

Document	Title
29.274	3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
29.281	General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
23.122	Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode
29.303	Domain Name System Procedures; Stage 3
29.501	5G System; Principles and Guidelines for Services Definition; Stage 3
23.501	System architecture for the 5G System (5GS)

3.2.1 LTE Architecture Model

The LTE EPS architecture includes many relevant network elements and interfaces to connect a User Equipment (UE) through the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) to the EPC. The key network elements in an EPC are:

- Mobility Management Entity (MME)
- Home Subscriber Server (HSS)
- Serving Gateway (SGW), and
- Packet Data Network Gateway (PGW).

Additionally, the Policy and Charging Rules Function (PCRF) is the entrance point to the Policy and Charging Control (PCC) architecture, but the specific functions of the PCC are outside the scope of the roaming architecture model.

The interfaces in a home EPC architecture are essentially the same as a roaming architecture with the only nuance being the labeling of the SGW and PGW interface. In a home architecture this interface is referred to as S5, while in a roaming architecture it is referred to as S8. Functionally, this interface is the same and signifies the extended path between a SGW and PGW, whereas in a home network these network elements may be co-located as an SGW/PGW. Figure 1 below shows a basic LTE EPS architecture model with a demarcation point reflecting the separation of the two Public Land Mobile Network (PLMN)s, termed as a Visited PLMN (VPLMN) and a Home (HPLMN).

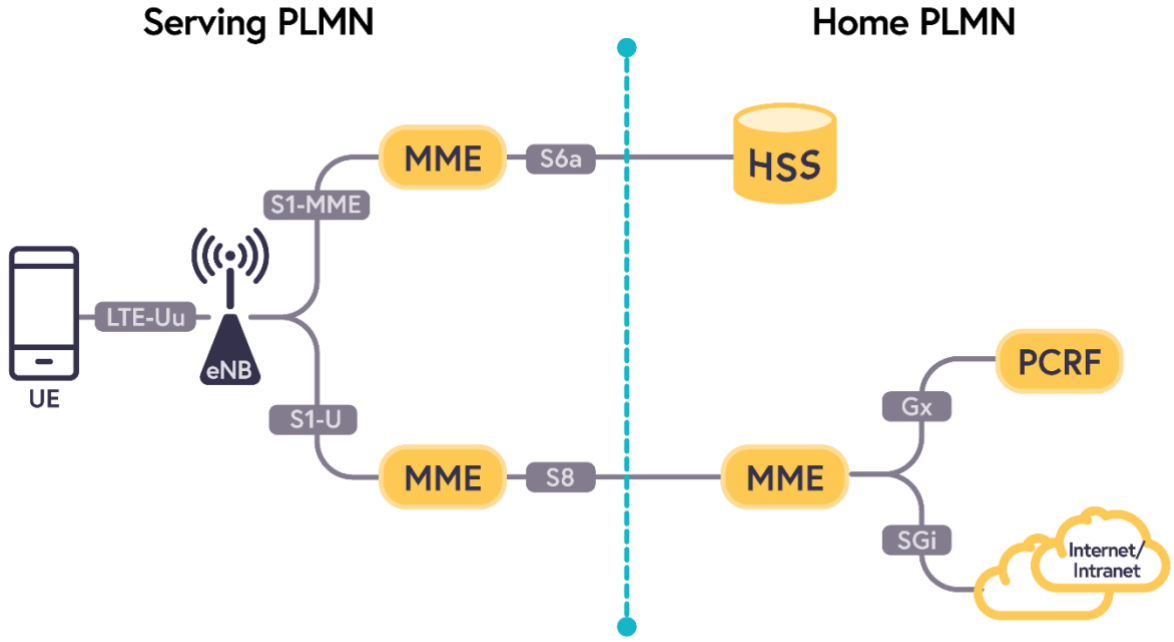

Figure 1: LTE Roaming Architecture

3.2.2 5G Architecture Model

The 5GS introduces a new RAN and Core that builds upon some of the techniques introduced within the iterations of previous generations. In the case of 5GS, this includes decoupling hardware from software allowing for the continual shift towards virtual network functions as well as further separating control plane (CP) and user plane (UP) functions to allow for greater independent scalability, among many other new capabilities. Because there is a new Core and RAN the 5GS introduces all new network elements and interfaces which are further described in [12].

The interfaces in a home 5GS architecture are essentially the same as a roaming architecture with the nuances being the introduction of the N32 interface for the Security Edge Protection Proxy (SEPP). The N32 interface will be HyperText Transfer Protocol 2 (HTTP2) based using Representational State Transfer (REST) based API calls between network functions. The N9 interface will continue to leverage the GPRS Tunneling Protocol (GTP) tunneling protocol between operator User Plane Function (UPF)s. An architecture model for 5G SA is depicted in Figure 2. Logical interfaces for nearly all network functions flow through the SEPP between a HPLMN and VPLMN except for the N9 interface for the UPF.

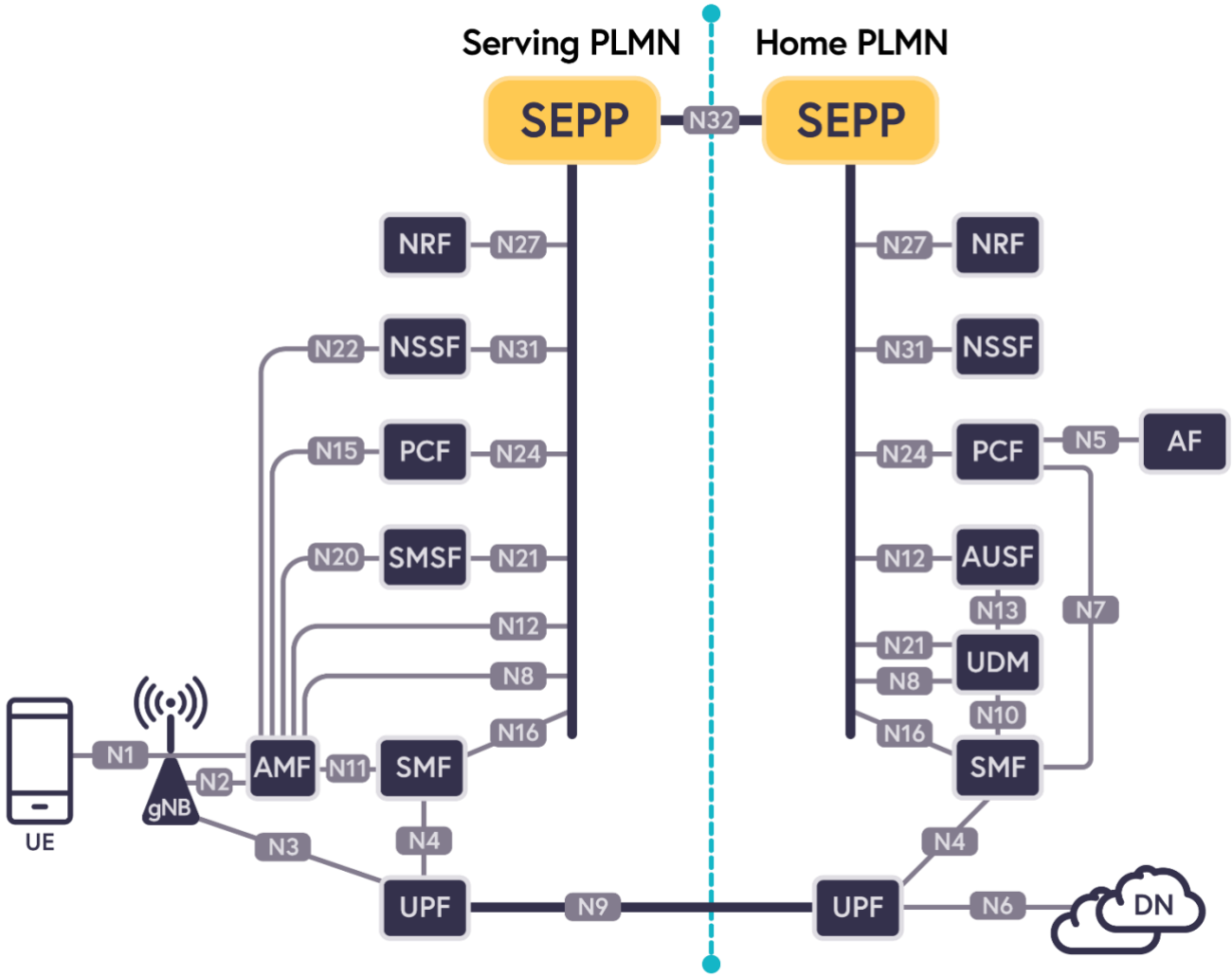

Figure 2: 5G Roaming Architecture

4 Interconnection Models

MNOs primarily leverage two methods for the interconnecting their networks for the purposes of supporting roaming and interconnect services. These options are leveraging third party, private interconnect services called IPX networks; or establishing direct private network connections between their networks.

4.1 eXchange (IPX)

As defined in the GSMA PRD IR.34 [13], the IPX Network is an inter-Service Provider IP backbone which comprises the interconnected networks of IPX Providers and GPRS Roaming eXchange (GRX) Providers. IPX is a telecommunications interconnection model developed by the GSMA for the support of roaming and interconnect traffic between service providers (MNOs, MSOs, etc.).

The IPX network is made up of several, interconnected IPX providers through the common Internet exchange (IX) Points to create a closed, private network that is isolated from the public internet. IPX providers must adhere to several GSMA standards and guidelines for providing IPX services. The main GSMA guideline for IPX providers is document titled IR.34 [13]; however, there are several others that address additional service requirements for IPX providers as well as service providers that connect to IPX. In addition to [13] the following guidelines in Table 2 are relevant to IPX providers and connected service providers:

Table 2: GSMA Guidelines for IPX

Doc	Title	Document Type	Working Group
IR.21	Roaming Database, Structure and Updating Procedures v15.1	Binding	Networks Group
IR.34	Guidelines for IPX Provider networks	Non-Binding	Networks Group
IR.40	Guidelines for IPv4 Addressing and AS Numbering for GRX/IPX Network Infrastructure and User Terminals	Non-Binding	Networks Group
IR.41	Definition of Quality-of-Service parameters and their computation		
IR.67	DNS Guidelines for Service Providers and GRX and IPX Providers	Non-Binding	Networks Group
IR.77	Inter-Operator IP Backbone Security Requirements	Non-Binding	Networks Group
IR.81	GRQ Measurement Implementation	Non-Binding	Networks Group
IR.88	LTE and EPC Roaming Guidelines	Non-Binding	Networks Group
IR.92	IMS Profile for Voice and SMS	Non-Binding	Networks Group
NG.113	5GS Roaming Guidelines	Non-Binding	Networks Group

The intent of IPX is to provide interoperability of IP services between all service provider types within a commercial framework that enables all parties in the value chain to receive a commercial return. The commercial relationships are underpinned with SLA which guarantee performance, quality, and security.

4.1.1 Network Addressing and Routing Requirements

Service providers that wish to utilize IPX services must adhere to the GSMA guidelines for network addressing and routing that are covered under GSMA guidelines in [13] and [14].

IPv4 addressing for any network hosts that must be reachable via IPX must be public, registered and not advertised or duplicated on the public internet. The use of IPv6 addressing can be supported on IPX provider's

networks between service providers where required by tunnelling the IPv6 traffic over IPv4. Both the IPX provider and service providers that utilize IPv6 within their networks must assume full responsibility for any/all network adjustments necessary for maintaining connectivity to all other IPX providers and/or service providers that deploy IPv4 addressing only.

The exchange of routing information between the IPX and connected service providers is via the use of Border Gateway Protocol (BGP). Service provider networks are considered an Autonomous System (AS) and are identified using an ASN to uniquely identify the network. The ASN is utilized to support the exchange of routing information between IPX providers and service providers. The ASN should be a public, registered ASN but if unavailable a private ASN assigned by the GSMA can utilized. However, the GSMA will only assign these private ASNs to GSMA members.

4.1.2 Class of Service

The IPX providers play an important role in ensuring that IP packets are routed and prioritized properly across their networks and between the connected service providers. This is critical to ensure that low latency applications such as VoLTE are provided priority should there be network routing or congestion issues.

The GSMA guidelines for Quality-of-Service/Class-of-Service (QoS/CoS) over IPX leverages Differentiated Services Field Codepoint (DSCP) or also referred to as DiffServ to mark the Type of Service (TOS) field in the IP packet header. Within the service providers EPS, the use of QoS Class Identifier (QCI) values are utilized to support QoS/CoS. Service providers connecting to the IPX map their EPS QCI values into IPX DSCP QoS values and mark the IP packets as they egress their network towards the IPX.

The following traffic classifications and mapping recommendations are defined within [13]:

Table 3: QCI Mapping

EPS QoS	GPRS/UMTS QoS Parameters		IP Transport		IPX QoS	Traffic Type Example
QCI	Traffic Class	THP	DiffServ PHB	DSCP	IPX Traffic Class	
1	Conversational	N/A	Expedite Forwarded (EF)	10110	Conversational	VoLTE, ViLTE
2						
3						
4	Streaming	N/A	Assured Forwarded (AF41)	100010	Streaming	Video Streaming
5	Interactive	N/A	Assured Forwarded (AF31)	011010	Interactive	Signaling, DNS
6			Assured Forwarded (AF21)	011100		Web browsing
7			Assured Forwarded (AF11)	001010		Instant Messaging
8	Background	N/A	Best Effort (BE)	000000	Background	Email, File Transfer

4.1.3 GSMA Domain Name System (DNS)

The IPX also provides essential functionality in DNS resolution. DNS services are critical to not only data roaming but also inter PLMN Multimedia Messaging Service (MMS) delivery and IP Multimedia Subsystem

(IMS) interworking between service providers. The IPX DNS is 100% separate from internet DNS and is formed using the GSMA Root DNS, Secondary Root DNS, and service provider Internal DNS. The Secondary Root DNS is typically provided by IPX providers for their connected service provider customers. However, a service provider could host Secondary Root DNS if they wish.

The GSMA Root DNS controls the Primary Zone File which has several inputs (IPX providers, service providers, etc.) and is policed by Neustar on behalf of the GSMA. The GSMA administers three domain names for the IPX and service providers to exchange traffic ensuring that VoLTE, Video over LTE (ViLTE), MMS, and Voice over Wi-Fi (VoWiFi) (calls, data, and messages) can be routed correctly. The three domains administered by the GSMA are .3gppnetwork.org, .gprs and .grx.

To ensure that the GSMA DNS data remains accurate the GSMA Root DNS and Secondary Root DNS are synchronized through a process known as a Zone Transfer. The below diagram depicts the zone transfer process.

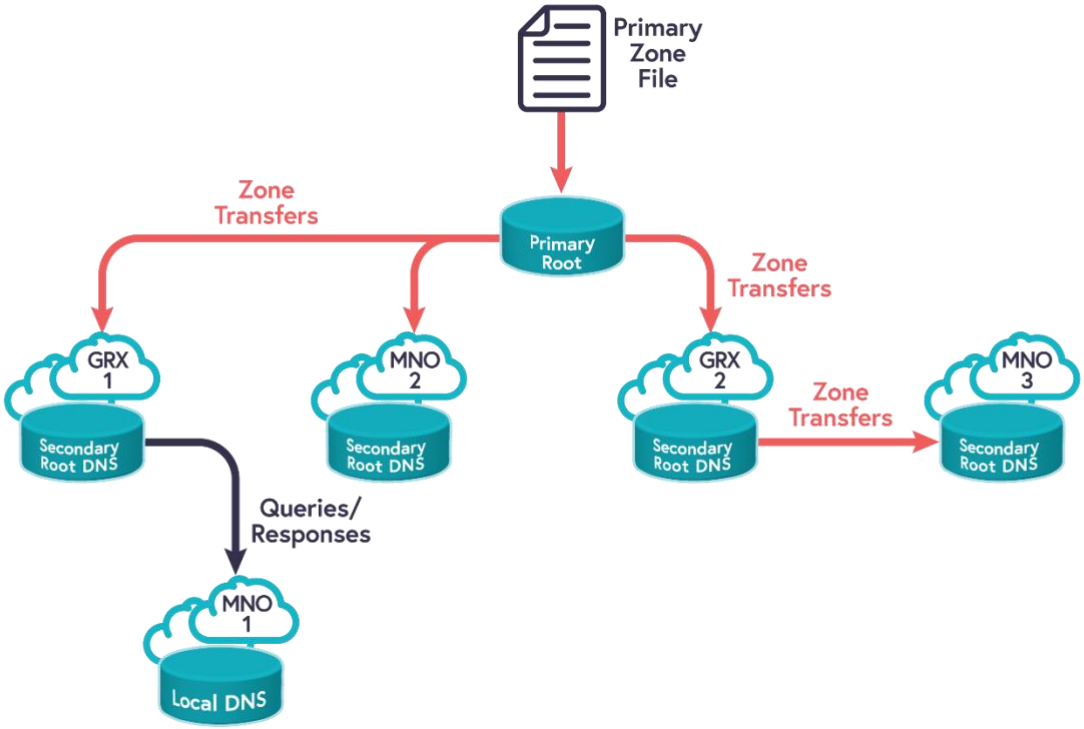

Figure 3: GSMA Root DNS and Secondary Root DNS

IPX providers in most cases provide the Secondary Root DNS and must support the transport of queries between their connected service providers and peered IPX providers to allow for correct resolution of a Fully Qualified Domain Name (FQDN) for all service requirements. Some examples of these FQDNs are APNs and Multimedia Messaging Service Centre (MMSC) hostnames (for MMS inter-working).

4.1.4 Service Level Agreement

IPX providers support end-to-end QoS requirements as per quality SLA as indicated in GSMA PRD IR.34 [13]. IPX providers create the peering agreements required with other IPX providers so that connections between IPX providers are implemented and managed by the IPX providers themselves based on the respective bi-

lateral SLAs. The QoS requirements for the IPX are outlined in the GSMA PRD IR.34, section 6 [13], and in the end-to-end QoS SLA description as per GSMA PRD AA.80 (IPX Agreement) [15]. It shall be noted that [15] is now a confidential document only available to GSMA members so reference is to an older publicly accessible version. IETF RFC 3246 [16] describes end-to-end QoS and is a mandatory requirement for IP Backbone Providers in the case of IPX.

The GSMA PRD AA.80 [15] describes the end-to-end QoS SLA describing connection models and the ways QoS are achieved, and its Section 6.1 outlines the concrete values for different class parameters. Furthermore, GSMA PRD AA.80 [15] Annex on the end-to-end SLA describes options for establishing physical connections from a Service Provider to the IPX categorized to Layer 1 connection (such as leased line or fiber optics), Layer 2 logical connection (such as 1 and 10 Gb/s Ethernet), and Layer 3 IP Virtual Private Network (VPN) connection over public IP network, the recommended option being IP Security (IPsec). In the SLA, Service Provider and IPX Provider need to consider the service guarantees for each IP QoS parameters, as well as responsibilities including help desk support and customer services. According to the GSMA PRD IR.34 [13], it is left to the discretion of IPX Provider and Service Provider to determine the details of each connection bilaterally and to agree the SLA.

4.1.5 Additional Services

IPX providers can also provide their customers with additional, value-added services above and beyond IPX transport. These services include but are not limited to the following:

- Diameter proxy, signaling & mediation
- Traffic policy & roaming controls
- Technology Interworking
- Network visibility tools
- Clearing & settlement
- Reporting

4.2 Direct Connection

The use of direct point-to-point network connections between MNOs is another means of interconnecting their networks in support of roaming traffic. In this model the two roaming partners order direct network transport facilities between their data centers.

Items like IP addressing, routing, class of service and APN resolution are handled uniquely between the service providers establishing the direct connection. Direct connections are often utilized in conjunction with IPX services since it is infeasible to directly connect to every roaming partner.

The direct connection between two mobile network operators can be realized by using a dedicated line or an IP tunnel over a public or private data network such as the Internet.

The dedicated line can be deployed applying available solutions such as Asynchronous Transfer Mode (ATM), Frame Relay (FR), or VPN tunnel. The benefit of the dedicated line is its capability to comply with the desired security and performance requirements of the interconnected MNOs. The most important drawback of the dedicated lines is their typically high cost especially in international environment when an MNO wants to deploy point-to-point lines with several counterparties. Furthermore, upon the onboarding of new roaming partners, their dedicated lines would need to be set up individually, which is time consuming.

The other alternative, an IP tunnel that interconnects two MNOs, can be based on a public data network such as the Internet via, e.g., IPsec. Nevertheless, applying this principle, it is challenging to comply with service level assurance by the very nature of the merely best effort performance of such networks.

Figure 4 depicts examples of the dedicated line and IPX. In this case, the MNO 1 and 2 have deployed IPsec on top of their selected direct connection whereas the MNO 1 also has reach-out to the MNO 3 and 4 via the IPX network.

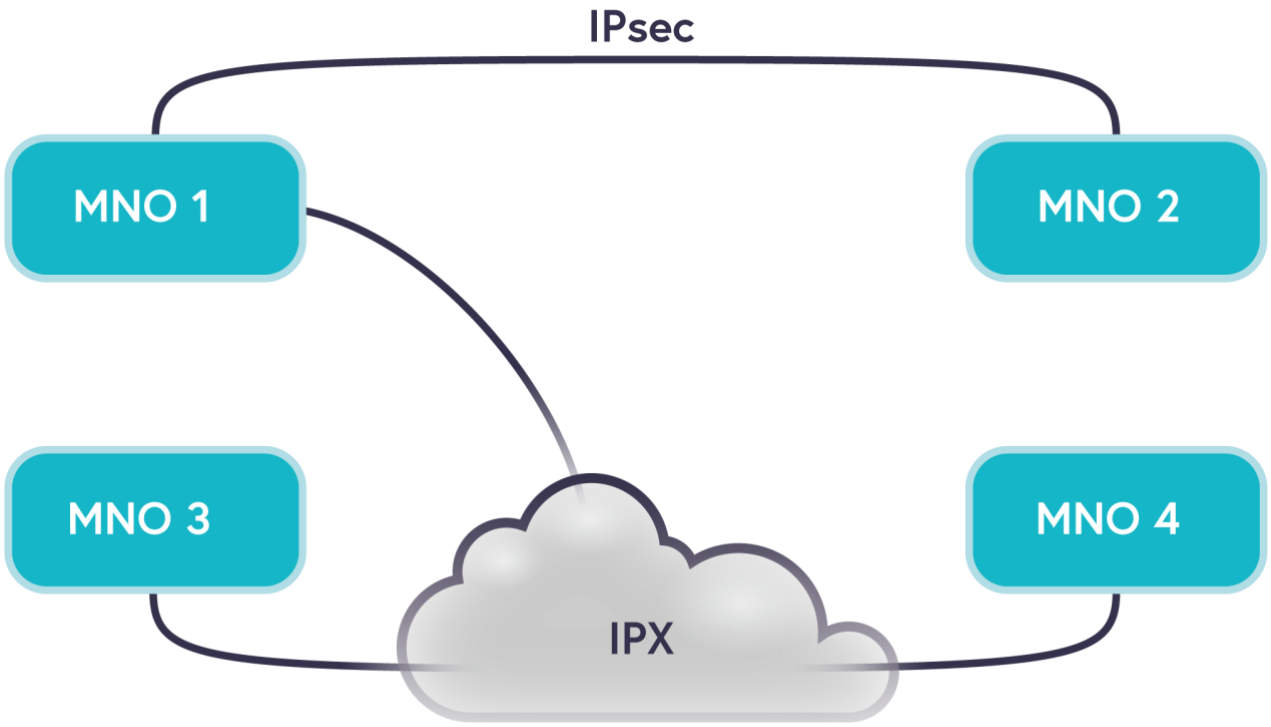

Figure 4: Example of Direct Roaming Connection Between MNO 1 and 2

5 Roaming Models

The primary concept of roaming is to enable mobility service while physically outside the range of a home RAN with a service experience that is similar or even identical. To achieve this capability, there must be some form of collaboration between a HPLMN and a VPLMN. There are multiple well defined architecture models to facilitate roaming, such as those described in [9] and [17] for an LTE system and [10] for a 5G system. Regardless of technology, the most common form of roaming is the Home Routed (HR) model which implies that signaling and user-plane data traffic are routed from a VPLMN back to the HPLMN for access to an internal or external network, e.g., an IMS or the public Internet. Additional roaming models include Local Breakout (LBO) and utilization of a Roaming Hub provider.

5.1 Standard roaming model with a dedicated PLMN ID

Before discussing the various roaming models, it is important to understand that traditionally, roaming implies that each VPLMN and HPLMN is using a dedicated MCC and MNC. There are some exceptions services within an operators' network, such as reseller, Mobile Virtual Network Operator (MVNO), Internet of Things (IoT), etc. but generally, MNOs engage in a direct roaming agreement as either unilateral or bilateral to enable roaming services for an entire PLMN at a time. An MNO with more than one PLMN Identifier (PLMN ID) that requires roaming access could negotiate to enable roaming access for all their MCC/MNC ranges at the same time with technical and billing validation occurring for each simultaneously, or sequentially depending on resource availability.

Contrary to this model, a private network operator is more likely to be using a PLMN ID that is shared among many different private network operators, which makes roaming a more challenging prospect. The following sections describe the standard roaming models at a high level, irrespective of PLMN ID, while sections 8 – 10 detail the key challenges of using a shared PLMN ID in these architecture models.

5.2 Home Routed (HR)

The term HR implies that the HPLMN operator controls the level of access and types of services available to their subscriber while roaming in a VPLMN. This includes all levels of signaling, such as Diameter for authentication and network registration as well as for data usage. This type of model allows a HPLMN to remain in the path of user-plane data for rating and charging purposes as well as to provide access to internal and external networks, such as for IMS services, and access to the public Internet from the subscriber's home country. While latency can become a factor for geographically dispersed MNOs this model is the most popular deployment model for the advantages of providing a home-like experience to subscribers.

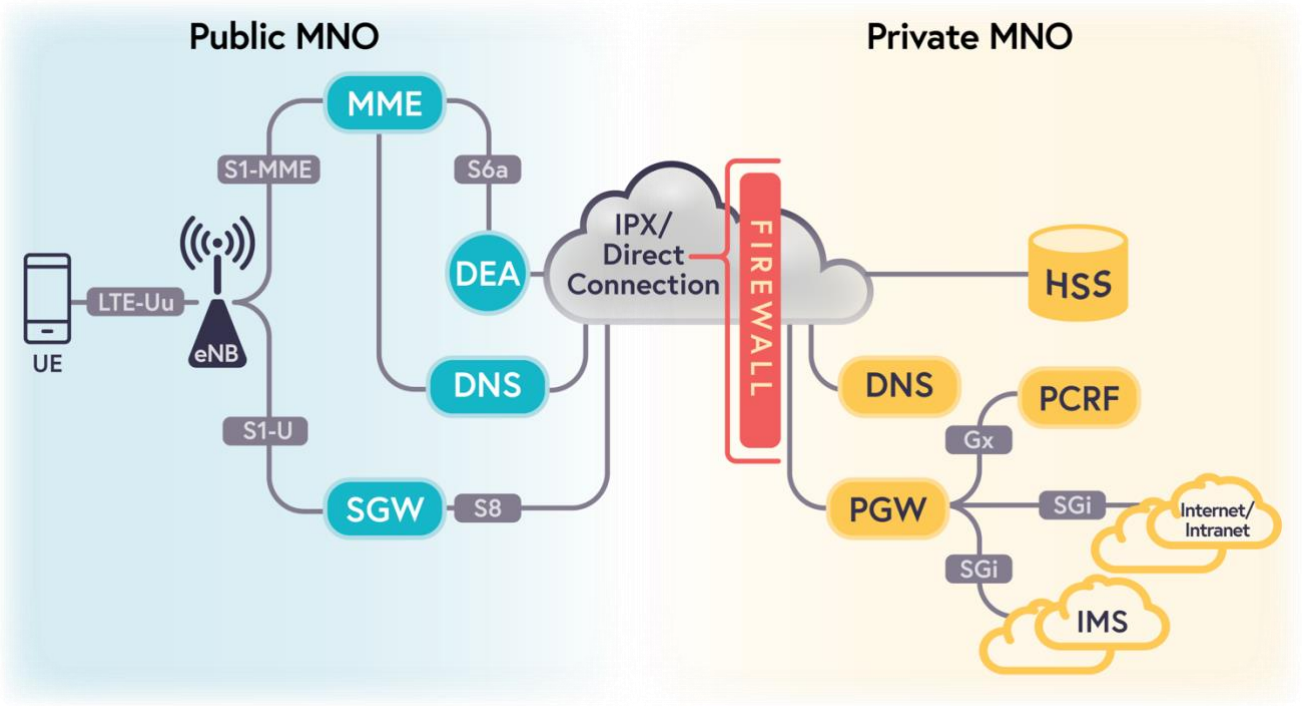

Figure 5: Generic Home Routed Architecture

5.3 Roaming Hub

A Roaming hub as described further in [18], is very similar in context to a HR architecture model, with the addition of an intermediary provider. The concept of a hub allows for faster entrance into roaming for smaller or newer operators that may be resource constrained and cannot dedicate the time and cost necessary to establish a global footprint of roaming agreements. The hub model creates the interconnection platform for a small MNO to quickly extend their reach and connectivity for a variety of signaling protocols covering GTP, SS7 and Diameter primarily.

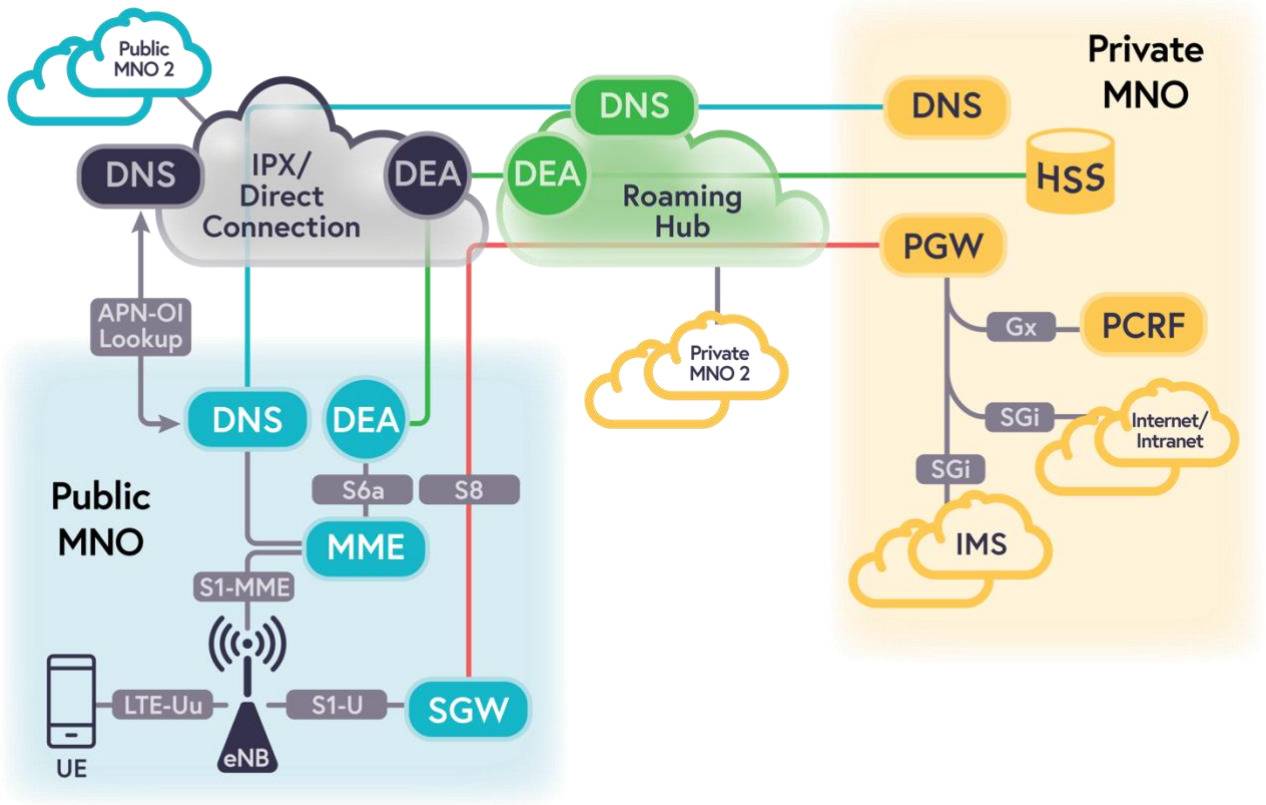

Figure 6: Generic Roaming Hub Architecture

5.4 Local Breakout (LBO)

Local Breakout as a roaming model is much less common across mobility networks than HR and Roaming Hubs but remains to be well defined in [9] and [17] for an LTE system and [10] for a 5G system. The key difference in an LBO vs. HR architecture is where the data session is anchored. In an LBO model, after authentication vectors and subscribed services are exchanged, the data session is anchored within the VPLMN instead of routed back to the HPLMN. This allows for a local content experience which can also mitigate any negative impacts from latency by routing data back to the HPLMN. There is an interface defined within the Policy and Charge Control (PCC) portion of an EPS for the exchange of policy rules and accounting records, but otherwise this model minimizes the volume of control plane messaging as well as eliminates the user-plane data that is routed over interconnection links for an APN that is allowed for LBO. The LBO model would involve more coordination between a HPLMN and VPLMN to enable roaming services, specifically regarding managing the data bearer and handling billing complexities.

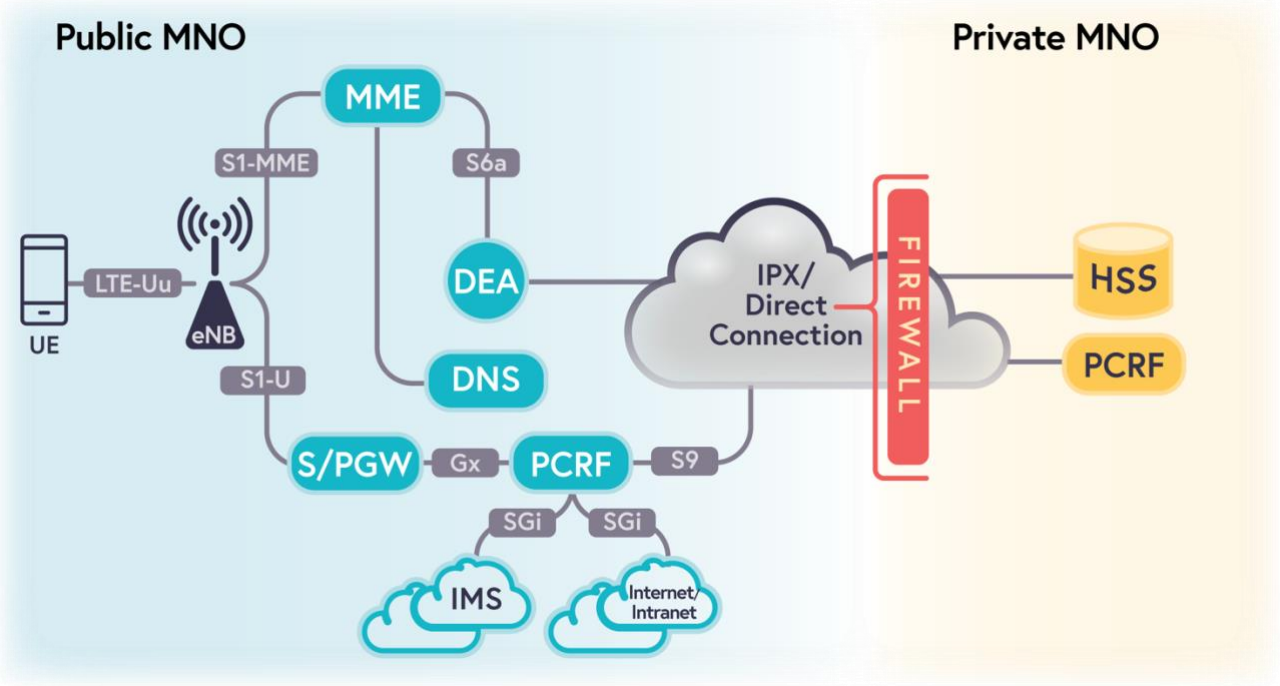

Figure 7: Generic Local Breakout Architecture

6 What is CBRS?

While wireless communication has become as essential as power, water, and internet connectivity for most organizations, wireless spectrum is finite, and increasingly scarce and valuable. The Citizens Broadband Radio Service (CBRS) reallocates spectrum for use by wireless networks and pioneers a new method for managing access to wireless spectrum. Established by the Federal Communications Commission (FCC) in April of 2015, it allocated 150 Megahertz (MHz) of spectrum from 3.55 to 3.7 Gigahertz (GHz) that had been previously reserved solely for military and other government-approved uses, for use by private organizations when not in active use by incumbent users. The FCC partitioned the band into 15 x 10 MHz channels, where access to the channels is dynamic and controlled by dedicated spectrum-management services known as the Spectrum Access System (SAS).

The OnGo Alliance created OnGo to promote the use of LTE and 5G in the 3.5 GHz band, though other technologies can also make use of the band. This is a high-level summary of some of the basics of CBRS and OnGo. For more information, we have multiple guides and whitepaper that give additional information available in [19].

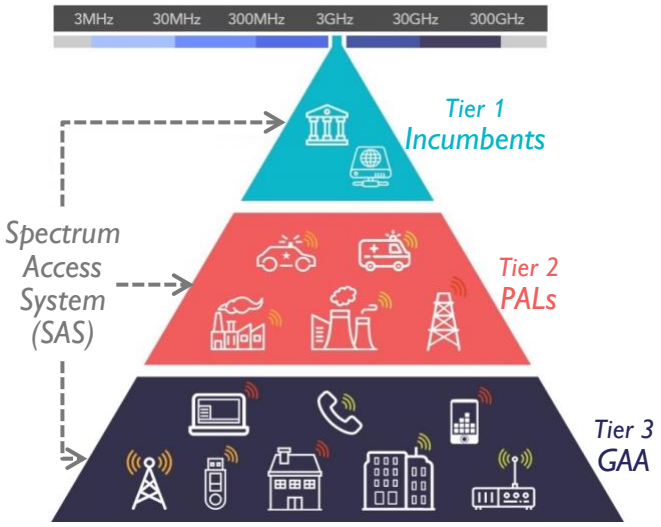

Figure 8: Spectrum Access System

6.1 The SASs

At the heart of dynamic spectrum sharing are the SAS. The SAS manages access to the CBRS band on a dynamic basis. Users of the band request access from a SAS, which grants access to specific channels, based on their tier.

- **Tier 1: Incumbents:** Top priority is given to defense radars and other grandfathered systems. When they need to use frequencies in the CBRS band, the SASs tell lower tier users to clear the channels in that area.
- **Tier 2: Priority Access License (PAL):** The FCC auctioned PALs to commercial users on a per county basis. Less than half (70 MHz) of the CBRS band was auctioned this way, with any single PAL user able to use up to 40 MHz of the band. Work is in progress to allow PAL sublicensing.
- **Tier 3: General Authorized Access (GAA):** GAA users are granted unprotected access to any spectrum that isn't being used by higher-tier networks.

There are multiple SAS providers, each administered by private companies. They coordinate between themselves when granting access to the band. Users that want to deploy a network in the CBRS band must contract with one of the SAS's to be granted access.

6.2 Citizens Broadband Radio Service Device

Non-mobile access points in CBRS are termed CBRS Devices (CBSD) in CBRS. CBSDs come in many types – fully integrated small-cells, distributed radio heads, or antenna clusters. CBRS defines a CBSD as a logical entity that radiates RF power, has antenna characteristics and is geolocated. CBSDs come in two classes, defined by their

output power, and range. Category A devices must emit less than one watt of power per 10 MHz channel. Category B devices, typically used outdoors, may emit up to 50 watts per 10 MHz channel. Broadly speaking, in an OnGo Network, the LTE eNodeB (eNB) and 5G gNodeB (gNB) are CBSDs. Technically, a CBSD is the point of transmission, so an eNB or gNB might have multiple CBSDs (one per cell or antenna). A list of OnGo certified CBSDs can be found in [20].

6.3 End User Device

In CBRS, the End User Device (EUD) is the user-facing element. These devices can be either mobile or fixed and their power can't exceed 23 dBm/10 MHz, 200 milliwatt (mW). EUDs may operate with permission from a CBSD. In an OnGo network, the EUDs are generally LTE and 5G UE devices. In the context of roaming to a commercial MNO a CBRS EUD must also include the ability to scan licensed bands for 4G or 5G in the country of operation. Within the United States, the FCC controls spectrum allocations and licensure for Mobile services and a private MNO should consult directly with a commercial MNO to ensure compatibility of EUDs.

6.4 OnGo and Support for CBRS

The OnGo Alliance is dedicated to supporting deployment of 3GPP networks, specifically, LTE and 5G New Radio (NR) in the CBRS band, which is called an OnGo network. The OnGo Alliance has not modified the air-interface of 3GPP networks, or any of the signaling between the UE and the eNB/gNB, so UEs that support band 48 (n48 in 5G) support OnGo with no modification or needed.

6.5 CBRS SHNI and OnGo Managed Identifiers

As discussed elsewhere in this document, both LTE and 5G NR networks are identified by their PLMN ID. PLMN IDs were intended to identify a small number of large networks, and there are not enough PLMN IDs available to support a large number of small networks. To address this issue, a MNC from within one of the USA MCCs was allocated for use by networks in the CBRS band. Therefore, the CBRS Shared Home Network Identifier (CBRS SHNI) is allocated the MCC/MNC of 315/010. An additional identifier, the CBRS Network Identifier (CBRS NID) is used to distinguish networks that use the CBRS SHNI. In LTE, the CSG-ID mechanism is used for the CBRS NID with the CBRS NID reported as the CSG ID. In 5G NR, we use the SNPN NID defined in Release 16 [21] to report the CBRS NID.

However, there are some problems that come along with using a SHNI; several identifiers used within LTE and 5G NR incorporate the PLMN ID to provide global uniqueness. If multiple networks are using the CBRS SHNI, these identifiers may not be globally unique, causing identifier collisions which can result in reduced performance, mobility failures, and denial of service. To prevent this, the OnGo Alliance administers an identifier management program, allowing network operators to obtain identifiers that are globally unique when using the CBRS SHNI. To achieve uniqueness, we have divided the Mobile Subscriber Identity Number (MSIN) component of the IMSI into a 4-digit IMSI Block Number (IBN), and a 5-digit user identification number. IBNs are assigned by the United States IMSI Administrator (ATIS), with the network operator able to issues up to 100,000 IMSIs per IBN. Additional information can be found in [22].

As discussed elsewhere in this document, the use of a CBRS SHNI also complicates roaming, as the PLMN ID of a network is not sufficient on its own to identify a network.

7 Understanding Needs, Use Cases, and Problems to be Solved

7.1 Use Case 1 - Shared HNI (Outbound) – Private-to-Public

After a firm decides on their specific needs for a OnGo-based private network they may have identified some devices that require mobility beyond the confines of the private RAN or potentially a need for backup connection capabilities from a commercial RAN. The number of EUDs, specific needs, and locations could vary but by establishing a roaming agreement with a commercial MNO a firm would gain added value and viability of the private core network capabilities. A firm that decides they need this extension capability understands the increases in latency that are possible in a roaming environment. As well, once a firm creates an external network connection they understand and accept the risks, roles, and responsibilities of complying with GSMA IR.77 [23] guidelines related to securing IPX external connections to one or more mobile network operators, or mutually agreed upon security requirements in a direct connect model. Example firms can range from those defined in the OnGo Private LTE Deployment Guide [24], such as the Smart-Building and Sports Venue to many others such as Smart Cities, Utility, Agriculture, Manufacturing and Tele-Health, among others. Enabling the capability to allow for access to Private Core Network data and applications without having to change SIM cards, end-user equipment, or expose those applications over the public Internet provides a valuable capability with potential for a global reach.

7.2 Use Case 2 - Shared HNI (Inbound Roaming) – Public-to-Private

A firm such as a Sports Venue, as detailed in the OnGo Private LTE Deployment Guide [24], or a shopping mall as described in the OnGo Neutral Host Network Deployment Guide [25], may have deployed a robust network with high levels of capacity covering a small geographic area and desires to recoup their capital expense by monetizing an inbound roaming capability. The leading architecture model for this capability would be a MOCN as described in the OnGo Neutral Host Network Deployment Guide [25], but an alternative or supplementary model would be to formally establish inbound roaming agreements through a traditional 3GPP based home routed or local breakout architecture [26]. This model allows for public MNO subscribers from multiple networks, beyond the limitations of the 6 unique PLMN IDs in a MOCN System [25] to roam into the OnGo Private RAN. This scenario could be optimal in areas where traditional commercial operator coverage is poor or non-existent such as in indoor, sporadic high-density, or rural areas.

7.3 Use Case 3 - Shared HNI (Inbound/Outbound Roaming) – Private-to-Private

Large enterprise organizations with multiple private core network locations such as a hospital system or retail property groups need the ability for some of their devices to gain access to each of their private installations without the added capital and operating expense of redundantly maintaining subscriber records across each private core, or the monetary costs and performance degradation of leveraging traditional roaming with a commercial MNO. Following a traditional 3GPP based architecture model as defined by 3GPP [26] for home routed or local breakout enables the ability for private network end users from within the same firm to seamlessly gain access to their private core and applications from within each private network installation.

8 Outbound Roaming - Home Routed

Outbound roaming using the HR model is a very popular method of deploying roaming services globally given the ability to provide subscribers with access to all the same carrier provided services that they would obtain in their home network. As well, a HR model allows the home MNO to maintain control at an individual subscriber level for which services are available to that subscriber during roaming. The following content describes how a HR model functions and where key challenges exist specifically for the CBRS SHNI. Figure 9 at the conclusion of this section depicts where key challenges exist as a visual reference to the HR architecture model.

From a public MNO standpoint, MME permissions to allow inbound roaming are commonly configured at the IMSI number series level, implying the MCC/MNC combination only. MME configuration that extends to incorporate the SHNI 4-digit IBN (MCC+MNC+IBN) could drastically increase the table size and may not be configurable in all MME vendor software variants. Verification of MME capabilities between a private and public MNO should be understood as a non-standard configuration, thus, support and acceptance of this as a standard approach to uniquely permit a SHNI MCC/MNC+IBN as a IMSI number series is a potential issue.

From a private network standpoint in the outbound roaming direction of a private network subscriber roaming on a public MNO, the HR model allows for the private core to control PGW allocation at a per APN level, meaning the private network PGW is the anchor point of the data session. This method allows for the private network to manage the data session, controlling IP allocation, QoS, and access to internal and external application servers among other functions. To achieve a HR architecture, a private network essentially needs to look like a public MNO and maintain a connection to partner operators using a method described in section 4, as well as follow similar levels of IR.21 network information exchange as described in section 3.1.1.

There are multiple signaling interfaces that need to be considered for a HR model, primarily the S6a interface for MME ⇔ HSS signaling, the S8 interface for session management and user plane data transfer, as well as DNS interconnection for APN resolution. For this architecture model it is required that the private EPC support these common roaming interfaces. The continuing sub-sections assume the roaming interfaces are supported in the private EPC.

8.1 Diameter Signaling

Diameter signaling for an EPS leverages the existing Diameter Base Protocol as defined in [27] and incorporates specific requirements for the S6a (MME ⇔ HSS) interface in [28]. Of key importance for signaling on the S6a interface in the outbound roaming direction is routing of a Diameter command code with the request flag set, such as Authentication Information (318), or Update Location (316) to the appropriate destination network based on a realm using the format epc.mncXXX.mcc.YYY.3gppnetwork.org as defined in [29]. Diameter routing within a public MNO and between interconnection points is facilitated through one or more diameter agents (DA) that maintain a Stream Control Transmission Protocol (SCTP) association between each DA and eventually to EPC network elements such as an MME and HSS.

It could be suggested that a private network would be small enough that Diameter end points, such as an MME and HSS, can associate directly. While that could be presumably common in a private network deployment, it would be uncommon for an MME in a large public MNO environment to associate directly to one or more HSS network elements. Within a public MNO, there is a likely a regional hierarchy of multiple DAs throughout the network for transmission of Diameter messages. At the edge of a public MNOs network a DA would facilitate the connection to external networks, commonly an IPX, or directly connected partner, and this network element is referred to as a Diameter Edge Agent (DEA). Fundamentally, the functions and connection methods

from a DEA are the same as a DA but would contain more specific route tables defined for destination-realms that exist externally from the public MNO.

As mentioned earlier, Diameter routing is commonly based on a well-defined format of a Destination-Realm. Therefore, one of the fundamental key issues outlined in [30] indicates that the Destination-Realm Attribute Value Pair (AVP) using the format defined in [29] be constructed solely from the SHNI cannot uniquely identify the exact home network without additional unique identification at a subscriber level.

The following sub-sections focus on the Authentication Information and Update Location command codes only. Additional Diameter command codes for the S6a interface related to an MME and HSS, such as Cancel Location (317) and Insert Subscriber Data (319) are documented in [28]. Diameter command codes for other interfaces in the EPS are outside the scope of this section.

8.1.1 Authentication

The Diameter command code for Authentication Information as defined in [28] facilitates the exchange of subscriber authentication vectors to be used over the S1 interface between an MME and UE during the initial attach or Tracking Area Update (TAU) procedure(s) defined in [26] as well as for periodic re-authentication procedures as needed. The routing of this command code is based on the Destination-Realm AVP using the format defined in [29] and as previously indicated, the Destination-Realm AVP constructed solely from the SHNI cannot uniquely identify the private network. However, the unique subscriber identifier within an Authentication Information Request (AIR) message is borrowed from [27] as the User-Name AVP and is a logical identifier that could be used for customizing the Destination-Realm at a DEA network element. This would require direct agreement between a private and public MNO and should be understood as a non-standard configuration, thus, support and acceptance of this as a standard approach to uniquely identify a SHNI destination network is a Public MNO choice.

Alternatively, the HSS FQDN could be leveraged as the destination-host to route Diameter signaling but the HSS FQDN is not known by an MME until after a successful Authentication Information Answer (AIA) is returned from an HSS which would include the origin-host AVP. As well, this HSS FQDN as a destination host is considered as optional in request messages and therefore is most likely ignored from a DEA route-table ruleset.

8.1.2 Update Location

The Diameter command code for Update Location as defined in [28] facilitates the validation of roaming permission and the exchange of subscribed services allowed for use in a VPLMN. A benefit of using a HR architecture for the roaming model means that a private MNO as a HPLMN can control on a per subscriber basis whether roaming in a VPLMN is allowed, and further, which services, including but not limited to APNs with associated QoS profiles, are allowed. The specific AVPs contained in an Update Location Request (ULR) are well defined within [28]. An HSS learns the MCC/MNC of the VPLMN that originated the ULR based on the VPLMN ID AVP and follows the format described in [28].

The routing of Diameter ULR messages and associated key issues for handling SHNI are the same as described for the Authentication Information procedures.

8.2 Access Point Name Resolution for Home Routed PDN Connections

APN resolution is a fundamental process for determining the PGW during initial attach procedures, as well as during subsequent stand-alone Packet Data Network (PDN) Connection Request procedures for UEs that require multiple data bearers. The APN resolution process within an EPS follows the well-defined Naming Authority Pointer (NAPTR) process defined in RFC 3403 and by 3GPP in [31], specifically using the straightforward-NAPTR (S-NAPTR) procedure. The S-NAPTR process allows for the authoritative Nameserver (NS) to provide a list of PGW candidates which can later be queried for their respective A record (IPv4) as described in [31]. It should be noted that in most roaming environments topology mapping is turned off and is therefore considered out of scope for this section.

The intent of this section is to focus on the APN resolution process as it relates to SHNI with some foundational background on APN structure and resolution procedures. It is important to be familiar with the EPS Session Management (ESM) procedures described in [26] for how a UE requests creation of a data bearer, as well as how an MME performs any necessary subscription validation of the requested bearer. Also, of note, is the APN Operator Identifier (APN-OI) Replacement AVP that is optionally included in the Diameter Update Location Answer (ULA) or Insert-Subscriber Data Request (IDR) which if supported in the HSS and MME can further influence the APN-OI portion of an APN.

8.2.1 APN Structure

As defined in [31] an APN is comprised of both a Network Identifier (APN-NI) and APN-OI through concatenation of a string of labels to form a FQDN. The APN-NI portion is commonly referred to simply as an APN but specifically represents the alphanumeric contents, potentially containing multiple labels, that are configured in the HPLMN HSS and PGW network elements as well as other necessary systems for data bearer management such as a PCRF. The APN-NI is also commonly configured within a UE although there are methods for the HSS to provide a default APN for data bearer creation and the UE could optionally not send the requested APN to the MME during the EPS Mobility Management (EMM) and ESM procedures defined in [26]. There are additional rules related to maximum length and disallowed character strings further defined in [29].

The APN-OI portion is constructed by an MME based on the MCC/MNC of the requesting IMSI, or optionally using the HSS APN-OI Replacement AVP using a standard format for each concatenated label as defined in [29]. The specific format of an APN-OI from [29] in an EPS takes the form of “mncXXX.mccXXX.3gppnetwork.org” where XXX are the values 0-9 from the MCC/MNC. In the case of a 2-digit MNC a leading 0 is always inserted. As well, the labels “apn.epc” are inserted between the APN-NI and APN-OI to form the APN FQDN as indicated in [29].

Both the APN-NI and APN-OI present challenges for a private MNO when attempting to use the HR model when roaming on a public MNO due to the lack of any subscriber specific information in the APN-NI portion as well as the fixed length of the MCC/MNC on the APN-OI portion. Ultimately, the entire APN FQDN must be unique and resolve only to a specific PGW(s) in the correct HPLMN. The APN-NI challenges can be overcome by each private MNO including a label that aligns to their IBN in the APN-NI portion and use that same APN in their HPLMN as well as when attempting to use a VPLMN.

APN-OI challenges are more difficult to overcome given the hierarchical structure of DNS resolution within GSMA based networks as described in section 4.1.3. To adapt to the GSMA structure for a SHNI, the Start of Authority (SOA) record would need to point towards a single entity, and no consideration of the APN-NI

label(s) would be used for identification of an authoritative NS. As a Public MNO choice, there are methods in DNS to maintain a local zone file or utilize DNS forwarding rules to leverage labels from the trailing end of the APN-NI in combination with the APN-OI to facilitate the forwarding of queries to a private MNO DNS. This would require direct agreement between a private and public MNO and should be understood as a non-standard configuration, thus, support and acceptance of this as a standard approach to uniquely identify a SHNI APN-OI is a Public MNO choice.

8.2.2 HSS APN-OI Replacement AVP

The APN-OI Replacement AVP is a HSS controlled parameter that can be set within the Subscription Data grouped AVP of the ULA or IDR messages. The value set within the APN-OI Replacement applies only to the APN it is directly associated to and serves to influence the APN-OI portion of an APN. Generally, for public MNOs this AVP would be used to modify the APN-OI to an MCC/MNC combination that is different from the IMSI, however in the case of a private MNO, if supported in both the HSS and MME, this AVP could inject a label that uniquely identifies the HPLMN. However, the same challenges presented in section 8.2.1 regarding SOA identification apply, as well, in practice, some public MNO MMEs may not have enabled support for the use of the APN-OI Replacement value. Therefore, this would require direct agreement between a private and public MNO to verify support before attempting to leverage this AVP to influence APN resolution.

8.2.3 IP Routing and Firewall

As recommended in [23] both MNOs and IPX providers should perform traffic filtering at their network edge. Within the public MNO space, this means that any RFC 1918 private addresses should be blocked as well as specific rule functionality to prevent source IP address spoofing need to be accounted for [23]. From a SHNI perspective the selected interconnection method, IPX or direct connection, will determine the extent of the access control list (ACL) provisioning as well as which application layer protocols should be allowed to follow the guidance from [23]. At minimum for S6a, DNS and S8 capabilities, the following ports and transport layer protocols should be permitted for the roaming partner IP ranges; DNS port 53 for both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), GTP ports 2123 and 2152 for UDP and Diameter using port 3868, or another agreed upon port, using SCTP should be permitted.

For a private network to interconnect with a public MNO through a IPX or direct connection the private network will need public, non-Internet routable IPv4 addresses for the roaming interfaces and functions such as DNS, S6a, and S8 that follow the network address and routing requirements detailed in section 4.1.1.

8.3 IP Multimedia Subsystem (IMS)

IMS refers to an additional core network that enables the ability for services, such as voice, Short Message Service (SMS), and video to use an IP based network as a replacement for circuit switched services. In some forums, IMS, and VoLTE or ViLTE are used synonymously but it is important to understand the distinction that VoLTE, ViLTE and SMS over IMS are services provided by an IMS core network as opposed to being a network themselves. IMS utilizes the well-established Session Initiation Protocol (SIP) and Real-Time Transport Protocol (RTP), among other protocols, for the exchange of datagrams between a client and server inside a MNOs network. The same protocols are always used in other common Voice over IP (VoIP) applications.

From a home routed model standpoint, IMS is a common service that enables the underlying VoLTE, SMS, and ViLTE services across MNO networks with the home IMS core of a subscriber handling the interconnection points to other public telephone networks for incoming and outgoing voice calls. There are alternative models

but in this section the focus is on the HR architecture, which is also commonly referred to as S8 Home Routed (S8HR) to signify the S8 interface connection network the VPLMN SGW and HPLMN PGW.

Given the model of a HR architecture implies transmitting all data back to the home core, it is implied that a private network would also need to deploy its own IMS core. For Voice based services the private network would also need to obtain telephone numbers from the appropriate numbering authority, such as the North American Numbering Plan Association (NANPA) in addition to interconnecting to one or more Local Exchange Carriers (LEC) and Long Distance (LD) carriers. IMS services are also more susceptible to latency, jitter, and packet delay; therefore, the interconnection model and bandwidth may need to be more robust than hosting other types of data applications. The UE requirements for IMS services, which include a SIP client using the appropriate parameters for the home MNO, are defined further in [32] but also represent a challenge given a wide range of device manufacturers.

8.3.1 Well-known IMS APN

Within the public MNO environment, it is understood and accepted that IMS services use the well-known APN of "IMS" [32]. This allows for QoS policy mapping to the appropriate QCI during session creation for the non-guaranteed bitrate (Non-GBR) bearer. Within [33] 3GPP indicates the non-GBR bearer for IMS Signaling is QCI 5, which also has one of the highest priority values, and therefore utilizing a standardized APN allows for more consistent alignment of QCI assignment between a MME, HSS and PCRF inside of a MNOs network as well as when S8HR is utilized.

The well-known IMS APN presents a challenge for SHNI based networks as the APN-NI portion cannot be used explicitly to identify a private network. Recall that the APN-OI portion has a fixed length for MCC/MNC digits as well, which preclude any possibly of manipulation to uniquely identify an SHNI entity by IBN. As well, the APN-NI portion offers the ability to append a label that uniquely identifies the SHNI entity and can be manipulated through HSS assignment or through APN-OI replacement. However, if this approach is used for the IMS APN, it would require direct agreement between a private and public MNO to support this new custom IMS APN variant. Therefore, it should be understood as a non-standard configuration. Support and acceptance of this as a standard approach to map a custom IMS APN to QCI 5 is a Public MNO choice. Some device manufacturers may also only support the well-known IMS APN and may require direct involvement to further understand if any non-standard customer IMS APN can be supported.

8.3.2 Over-The-Top (OTT)

An alternative to EPS provided IMS services for a private network includes the use of commercially available or enterprise specific over-the-top (OTT) applications. An OTT solution for real-time exchange of VoIP allows for flexibility and simplicity if a private network does not have the ability or desire to maintain a dedicated IMS core. For OTT solutions that run as standalone applications using a UE's data browsing APN, it is possible for a private network entity to contract with a 3rd party to host IMS services. However, the nuances of a hosted IMS service as it applies to a HR architecture model is outside the scope of this section.

8.4 Key Issues for Outbound Roaming – Home Routed

Home routing traffic presents numerous challenges for both a private and a public MNO. While some of the key issues are reconcilable through direct agreement for non-standard handling, others require further evaluation. The architecture of a home-routed solution is shown in the following figure, with the labelled items briefly discussed in the following list.

Outbound Roaming – Home Routed

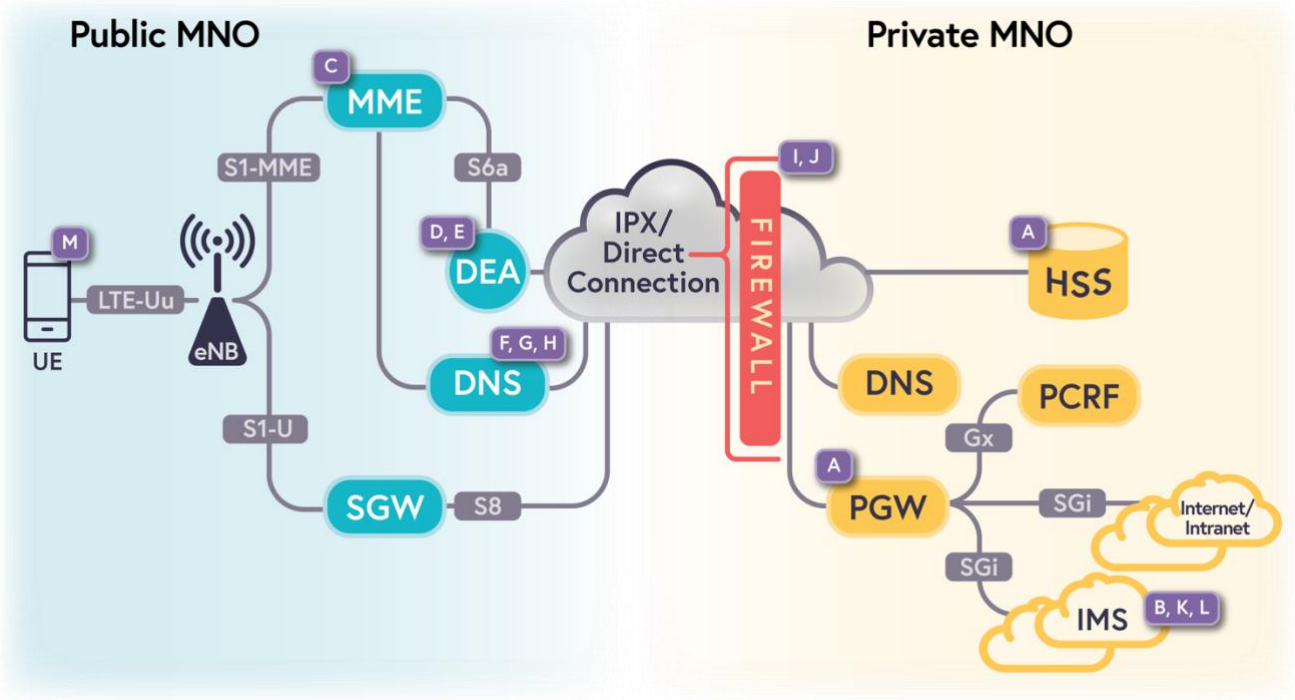

Figure 9: Key Issues for Outbound Roaming – Home Routed

Throughout this section the following key issues (not listed in priority order) shown in the above diagram have been raised for awareness purposes only:

- A **Private EPC:** Roaming interfaces for S6a and S8 must be supported in the Private EPC.
- B **Private EPC:** S8HR IMS services require the private core must have its own IMS core.
- C **Public MNO MME:** MME permissions may not be configurable beyond 5 or 6 digits to incorporate the SHNI MCC/MNC+IBN combination.
- D **Public MNO Diameter:** There is no SHNI indicator in the destination realm for Diameter routing.
- E **Public MNO Diameter:** User-Name AVP routing is non-standard.
- F **Public MNO DNS:** The APN FQDN does not contain any subscriber specific indication unless a label is included by a private MNO, in which there is no regulatory body to prevent duplication.
- G **Public MNO DNS:** Root DNS records for a SHNI APN-OI would need to point to a common entity as the SOA record.
- H **Public MNO DNS:** APN-OI Replacement may not be universally supported in public MNO MMEs.
- I **IPX/Direct Interconnection:** The private MNO must use Public, non-Internet routable IPv4 addresses as well as a unique ASN for BGP peering and interconnection.
- J **Private MNO Firewall:** The private MNO would need to configure and maintain firewall rules for the connected Public MNO(s) backbone IP ranges and associated ports for DNS, Diameter and GTP traffic.
- K **Numbering:** A private network offering IMS services would need to obtain telephone numbers from the appropriate numbering authority.

Outbound Roaming – Home Routed

L **IMS Interworking:** IMS services are more susceptible to latency, jitter, and packet delay therefore, the interconnection model and bandwidth may need to be more robust than hosting other types of data applications. IMS Core would need to interwork with LEC/LD providers.

M **Private MNO UE:** For IMS to be supported, the private MNO UE could need a custom SHNI+IBN SIP client.

9 Outbound Roaming – Hub

Outbound roaming using a Hub model is a less common method of deploying roaming services compared to HR. Comparatively to outbound roaming using a HR model, a Roaming Hub allows a private network the ability to provide subscribers with access to a similar suite of services to those provided within their home network. As well, a Roaming Hub model allows the home MNO control for which public MNO network roaming services are allowed [18]. From a private network community perspective, a Roaming Hub model addresses some of the inherent challenges presented using a SHNI as well as reduces the level of effort to establishing a global footprint by allowing a single entity to create the necessary roaming relationships with public MNOs [18]. Figure 10 at the conclusion of this section depicts where key challenges exist as a visual reference to the Roaming Hub architecture model.

From a public MNO standpoint, a Roaming Hub provider representing SHNI enterprises allows for a more standard configuration of roaming services. For example, MME permissions to allow inbound roaming are commonly configured at a IMSI number series level, implying the MCC/MNC combination only. MME configuration that extends to incorporate the SHNI 4-digit IBN (MCC+MNC+IBN) could drastically increase the table size as well as may not be configurable in all MME vendor software variants. Unique permissions at a SHNI MCC/MNC+IBN level as a IMSI number series is a potential issue in other roaming architecture models. With a Roaming Hub model, a public MNO could configure MME permissions at the MCC/MNC level thus mitigating this challenge. Control of which enterprises can access that public MNO is then passed to the Roaming Hub provider. While the MME configuration is streamlined, there is an inherent risk to Key Performance Indicator (KPI) by allowing the entire MCC/MNC of a SHNI as it could potentially also allow attach attempts for SHNI enterprises that are not allowed to roam through the hub.

The Roaming hub model creates design considerations that can affect the underlying architecture for the common roaming interfaces, such as S6a, S8 and for APN resolution. For a SHNI, a single Roaming Hub provider would be required to achieve the greatest benefit. If there were multiple Roaming Hub providers for the SHNI the issues and challenges related specifically to HR would reoccur. For the purposes of this section, it is assumed the roaming hub hosts each of these interfaces for the interconnection to a Public MNO and can support a combination of one or more to the S6a, S8 and DNS interfaces connection to a private MNO, if supported by the private MNO, or alternatively host the HSS, DNS and PGW functions on behalf of the private MNO. Where appropriate in the following sections the interconnection options from a Roaming Hub to a private MNO will be identified and compared with hosted EPC options.

9.1 Diameter Signaling

Diameter signaling for an EPS leverages the existing Diameter Base Protocol as defined in [27] and incorporates specific requirements for the S6a (MME ⇔ HSS) interface in [28]. Of key importance for signaling on the S6a interface in the outbound roaming direction is routing of a Diameter command code with the request flag set, such as Authentication Information (318), or Update Location (316) to the appropriate destination network based on a realm using the format epc.mncXXX.mcc.YYY.3gppnetwork.org as defined in [29]. Diameter routing within a public MNO and between interconnection points is facilitated through one or more DA that maintain a SCTP association between each DA and eventually to EPC network elements such as an MME and HSS.

Commonly in a public MNO, there is a regional hierarchy of multiple DAs throughout the network for transmission of Diameter messages. While presumably common in a private network deployment, it would be uncommon for an MME in a large public MNO environment to associate directly to one or more HSS network elements. At the edge of a public MNOs network a DA would facilitate the connection to external networks,

commonly an IPX, or directly connected partner, and this network element is referred to as a DEA. Fundamentally, the functions and connection methods from a DEA are the same as a DA but would contain more specific route tables defined for destination-realms that exist externally from the public MNO.

One of the fundamental key issues outlined in [30] indicates that the Destination-Realm AVP using the format defined in [29] constructed solely from the SHNI cannot uniquely identify the exact home network without additional unique identification at a subscriber level. However, a Roaming Hub model mitigates this concern at the Public MNO by allowing sustainment of existing DEA routing configuration, in alignment with the realm format in [29]. Eventually, within the route from MME to HSS the SHNI the explicit private MNO must be identified but a DA within the Roaming Hub provider is the most logical appliance to handle any necessary traffic diversion based on the SHNI.

The following sub-sections focus on the Authentication Information and Update Location command codes only. Additional Diameter command codes for the S6a interface related to an MME and HSS, such as Cancel Location (317) and Insert Subscriber Data (319) are documented in [28]. Diameter command codes for other interfaces in the EPS are outside the scope of this section.

9.1.1 Authentication

The Diameter command code for Authentication Information as defined in [28] facilitates the exchange of subscriber authentication vectors to be used over the S1 interface between an MME and UE during the initial attach or TAU procedure(s) defined in [26] as well as for periodic re-authentication procedures as needed. The routing of this command code is based on the Destination-Realm AVP using the format defined in [29] and therefore in a Roaming Hub Model a Public MNO can route towards an IPX based on the standard realm format, regardless of which enterprise the specific SNHI belongs to. Through interconnection to an IPX, a Roaming Hub provider could then perform a further inspection of the AIR at a DA and direct the message to the enterprise specific HSS, if a S6a interconnection exists. The SHNI identification could be achieved through the User-Name AVP, which is borrowed from [27], and offers the most logical information element to perform the unique subscriber identification within an AIR.

Alternatively, if a private MNO EPS does not support the S6a roaming interface a direct agreement could be reached to host the HSS service for the private MNO, which would also then require the Roaming Hub HSS to be involved in all authentication attempts inside the private MNO EPS as well as when roaming in a public MNO VPLMN. Whether the HSS function is hosted or connected via an S6a interface, the Roaming Hub would require interconnection to one or more IPX providers to achieve global reach within minimal IPX hops involved.

9.1.2 Update Location

The Diameter command code for Update Location as defined in [28] facilitates the validation of roaming permission and the exchange of subscribed services allowed for use in a VPLMN. A benefit of using a Roaming Hub model is that the subscribing private MNO as a HPLMN can control on a per public MNO basis whether roaming in a VPLMN is allowed [18]. Additionally, the services, including but not limited to APNs with associated QoS profiles, that are allowed could be controlled on a per subscriber basis. The potential for subscriber level control exists regardless of whether the private MNO maintained an S6a interface connection to the Roaming Hub provider, of if the Roaming Hub provider hosted the HSS.

The specific AVPs contained in a ULR are well defined within [28]. An HSS learns the MCC/MNC of the VPLMN that originated the ULR based on the VPLMN ID AVP and follows the format described in [28]. The routing of

Diameter ULR messages and associated key issues for handling SHNI are the same as described for the Authentication Information procedures.

9.2 Access Point Name Resolution for Roaming Hub PDN Connections

APN resolution is a fundamental process for determining the PGW during initial attach procedures, as well as during subsequent stand-alone PDN Connection Request procedures for UEs that require multiple data bearers. The APN resolution process within an EPS follows the well-defined NAPTR process defined in RFC 3403 and by 3GPP in [31], specifically using the S-NAPTR procedure. The S-NAPTR process allows for the authoritative NS to provide a list of PGW candidates which can later be queried for their respective A record (IPv4) as described in [31]. It should be noted that in roaming environments topology mapping is turned off and is therefore considered out of scope for this section.

The intent of this section is to focus on the APN resolution process as it relates to SHNI with some foundational background on APN structure and resolution procedures. It is important to be familiar with the ESM procedures described in [26] for how a UE requests creation of a data bearer, as well as how an MME performs any necessary subscription validation of the requested bearer. Also, of note, is the APN-OI Replacement AVP that is optionally included in the Diameter ULA or IDR which if supported in the HSS and MME can further influence the APN-OI portion of an APN.

9.2.1 APN Structure

As defined in [29] an APN is comprised of both an APN-NI and APN-OI through concatenation of a string of labels to form a FQDN. The APN-NI portion is commonly referred to simply as an APN but specifically represents the alphanumeric contents, potentially containing multiple labels, that are configured in the HPLMN HSS and PGW network elements as well as other necessary systems for data bearer management such as a PCRF. The APN-NI is also commonly configured within a UE although there are methods for the HSS to provide a default APN for data bearer creation and the UE could optionally not send the requested APN to the MME during the EMM and ESM procedures defined in [26]. There are additional rules related to maximum length and disallowed character strings further defined in [29].

The APN-OI portion is constructed by an MME based on the MCC/MNC of the requesting IMSI, or optionally using the HSS APN-OI Replacement AVP using a standard format for each concatenated label as defined in [29]. The specific format of an APN-OI from [29] in an EPS takes the form of “mncXXX.mccXXX.3gppnetwork.org” where XXX are the values 0-9 from the MCC/MNC. In the case of a 2-digit MNC a leading 0 is always inserted. As well, the labels “apn.epc” are inserted between the APN-NI and APN-OI to form the APN FQDN as indicated in [29].

Both the APN-NI and APN-OI present challenges for a private MNO when attempting to use the Roaming Hub model for roaming on a public MNO due to the lack of any subscriber specific information in the APN-NI portion as well as the fixed length of the MCC/MNC on the APN-OI portion. Ultimately, the entire APN FQDN must be unique and resolve only to a specific PGW(s) in the correct HPLMN or potentially in the Roaming Hub PGW, if used. The APN-NI challenges can be overcome by each private MNO including a label that aligns to their IBN in the APN-NI portion and use that same APN in their private EPC as well as when attempting to use a VPLMN. Alternatively, in a Roaming Hub, a provider of the Hub could inspect the GTP Create Session Request (CSR) message and decide based on the IMSI the real private MNO for redirection of the CSR to the private MNO PGW (if an S8 interface exists) or for further GTP user plane (GTP-U) management.

APN-OI challenges are less difficult to overcome in a Roaming Hub model given the hierarchical structure of DNS resolution within GSMA based networks as described in section 4.1.3. To adapt to the GSMA structure for a SHNI, the SOA record would need to point towards a single NS residing in the Roaming Hub provider and thus no consideration of the APN-NI label(s) would be necessary for identification of a private MNO authoritative NS from a public MNO. The Roaming Hub DNS involvement in the APN resolution process then more closely follows the functionality with a public MNO environment where each MNO uses a dedicated MCC/MNC.

9.2.2 GSMA Root DNS

The best practices referenced in section 4.1.3 can more easily be followed in a Roaming Hub model than other outbound roaming architectures, as the Roaming Hub provider could indicate itself as the authoritative NS for the SHNI APN-OI. This would allow all global roaming partners with an established agreement to the Roaming Hub to know through IR.21 exchange, or through GSMA Root DNS lookup procedures, that the Roaming Hub DNS is the SOA. There is a design consideration for a Roaming Hub provider and private MNOs to determine which entities PGW would be the anchor point for data sessions when roaming, and if the Roaming Hub provider hosted PGW services, it would be unnecessary to manage an extensive name database (named) presuming the Roaming Hub provider was also managing the sessions based on IMSI. As well, it would then be less important to force uniqueness within the APN-NI, although that is likely still a best practice.

Alternatively, a Roaming Hub provider could perform zone transfers with a local authoritative DNS in each private MNO, meaning the APN-NI must be unique. This design choice complicates the DNS processes and assumes there is an interconnection point for DNS traffic between the Roaming Hub and private MNO, as well as for the S8 interface. This approach would however allow for the PGW in the private MNO to be the anchor point for an EPS bearer and more closely mimic a HR model for roaming. If this model is chosen, there are additional design complexities as it relates to the exchange of PGW IP addresses between the public and private MNOs, through the Roaming Hub provider.

9.2.3 HSS APN-OI Replacement AVP

The APN-OI Replacement AVP is a HSS controlled parameter that can be set within the Subscription Data grouped AVP of the ULA or IDR messages. The value set within the APN-OI Replacement applies only to the APN it is directly associated to and serves to influence the APN-OI portion of an APN. Generally, for public MNOs this AVP would be used to modify the APN-OI to an MCC/MNC combination that is different from the IMSI, however in the case of a private MNO, if supported in both the HSS and MME, this AVP could inject a label that uniquely identifies the HPLMN or Roaming Hub provider.

However, the same challenges presented in section 9.2.1 regarding SOA identification apply, as well, in practice, some public MNO MMEs may not have enabled support for the use of the APN-OI Replacement value. Therefore, this would require direct agreement between a Roaming Hub and public MNO to verify support before attempting to leverage this AVP to influence APN resolution.

9.2.4 IP Routing and Firewall

As recommended in [23] both MNOs and IPX providers should perform traffic filtering at their network edge. Within the public MNO space, this means that any RFC 1918 private addresses should be blocked as well as specific rule functionality to prevent source IP address spoofing needs to be accounted for [23]. From a Roaming Hub model perspective, the design choice of whether the Roaming Hub will host PGW services or if

there would be an S8 interface between the Roaming Hub and private MNO determines the complexities of the IP routing and firewall policies.

The easier model to follow would be for the Roaming Hub provider to host PGW services on behalf of the private MNO, at which point it would be necessary for the Roaming Hub provider to maintain one or more IPX connections for global connectivity as well as would need to follow the best practices in [23] for managing firewall permissions. Ideally, the Roaming Hub would establish roaming agreements globally for the SHNI MCC/MNC and in the IR.21 exchange would provide the public, non-routable, IP, addresses of its PGW.

A more complicated model would include the private MNO also maintaining an IPX connection, or at minimum a direct connection to the Roaming Hub provider and at the time of onboarding share the private MNO PGW IP ranges to be announced on the Roaming Hub providers IR.21. Additionally, the launch timelines and increased risk of routing problems would occur given the timelines permitted for public MNOs to configure routing permissions and firewall policies as indicated in section 4.1.1.

Once a Roaming Hub design decision is made, the entity providing the PGW services would need to maintain the ACL provisioning as well as which application layer protocols should be allowed to follow the guidance from [23]. At minimum for S6a, DNS and S8 capabilities, the following ports and transport layer protocols should be permitted for the roaming partner IP ranges; DNS port 53 for both TCP and UDP, GTP ports 2123 and 2152 for UDP and Diameter using port 3868, or another agreed upon port, using SCTP should be permitted.

9.3 IMS

IMS refers to an additional core network that enables the ability for voice, SMS, and video to use an IP based network as a replacement for circuit switched service. Commonly, IMS and VoLTE or ViLTE are used synonymously but it is important to understand the distinction that VoLTE, ViLTE and SMS over IMS are services provided by an IMS core network as opposed to being a network themselves. IMS utilizes the well-established SIP and RTP, among other protocols, for the exchange of datagrams between a client and server inside a MNOs network. The same protocols are always used in other common VoIP applications.

The Roaming Hub model complicates IMS more so than in other roaming models. Specifically, IMS enables the ability for a UE to use VoLTE, ViLTE, and SMS over IMS regardless of location, and in the roaming case, the HR model is the most common. If a private MNO desires to have IMS services available inside the private EPS, this insinuates either the private MNO EPS includes a separate IMS core, or they have agreed with a 3rd party to host an IMS core. For the addition of roaming, there is potential for S8 redirection through a Roaming Hub to the private MNO, but previously mentioned design considerations must also then be met, such as S8 interface capability, interconnection, IP route advertisement exchange, firewall management, and APN resolution. If a Roaming Hub hosted IMS services for the private MNO this simplifies some of the complexities from a roaming standpoint but would then require interconnection to be in place with enough bandwidth to handle the IMS volume from within the private MNO RAN.

Regardless of whether a Roaming Hub hosted IMS for a private MNO or facilitated a hybrid S8HR type model for traffic redirection to the private MNO there is still a requirement to obtain telephone numbers from the appropriate numbering authority, such as the NANPA in addition to interconnecting to one or more LEC and LD carriers. Additionally, the UE requirements for IMS services, which include a SIP client using the appropriate parameters for the home MNO, or hosted IMS solution also represent a challenge given a wide range of device manufacturers. Further UE requirements for IMS are defined further in [32].

9.3.1 Well-known IMS APN

Within the public MNO environment, it is understood and accepted that IMS services use the well-known APN of "IMS" [32]. This allows for QoS policy mapping to the appropriate QCI during session creation for the Non-GBR bearer. Within [33], 3GPP indicates the non-GBR bearer for IMS Signaling is QCI 5, which also has one of the highest priority values, and therefore utilizing a standardized APN allows for more consistent alignment of QCI assignment between a MME, HSS and PCRF inside of a MNOs network as well as during roaming scenarios.

The well-known IMS APN presents a challenge for SHNI based networks as the APN-NI portion cannot be used explicitly to identify a private network. Recall that the APN-OI portion has a fixed length for MCC/MNC digits as well, which preclude any possibly of manipulation to uniquely identify an SHNI entity by IBN. As well, the APN-NI portion offers the ability to append a label that uniquely identifies the SHNI entity and can be manipulated through HSS assignment or through APN-OI replacement. However, if this approach is used for the IMS APN, it would require direct agreement between a private and public MNO to support this new custom IMS APN variant. Therefore, it should be understood as a non-standard configuration. Support and acceptance of this as a standard approach to map a custom IMS APN to QCI 5 is a Public MNO choice. Some device manufacturers may also only support the well-known IMS APN and may require direct involvement to further understand if any non-standard customer IMS APN can be supported.

The Roaming Hub model combined with a hosted IMS service from the Hub provider presents an opportunity to mitigate the challenges of APN resolution if the ability to manage sessions based on the IMSI are available. A Roaming Hub model combined with a private MNO IMS core though re-introduces some of the APN complexity depending on the eventual design of the interconnection between the public MNO, Roaming Hub provider and private MNO.

9.3.2 OTT

An alternative to EPS provided IMS services for a private network includes the use of commercially available or enterprise specific OTT applications. An OTT solution for real-time exchange of VoIP allows for flexibility and simplicity if a private network does not have the ability or desire to maintain a dedicated IMS core.

9.4 Key Issues for Outbound Roaming - Hub

The use of a Roaming Hub presents alternatives to the HR model and while mitigating some challenges it can introduce additional complexities for both a private and a public MNO. While some of the key issues are reconcilable through direct agreement for non-standard handling, others require further evaluation. The architecture of a hub solution is shown in the following figure, with the labelled items briefly discussed in the following list.

Outbound Roaming – Hub

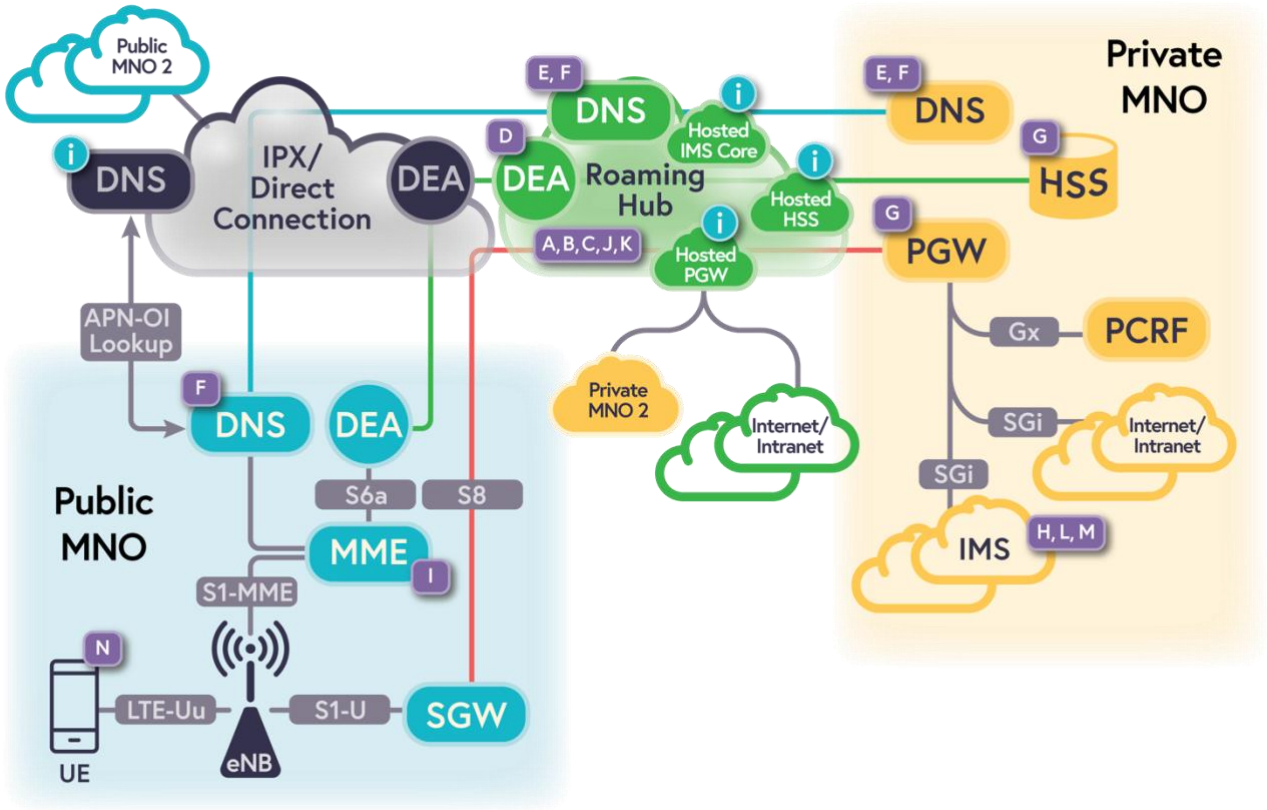

Figure 10: Key Issues for Outbound Roaming – Hub

Throughout this section the following key issues (not listed in priority order) shown in the above diagram have been raised for awareness purposes only:

- A **Roaming Hub:** The Hub provider must inter-connect to public MNOs via IPX.
- B **Roaming Hub:** The Hub provider must establish and launch roaming agreements for the SHNI.
- C **Roaming Hub:** A single provider should host the hub function for the entire SHNI.
- D **Roaming Hub:** User-Name AVP based routing is required.
- E **Roaming Hub:** DNS zone transfers or similar solution may be required if Hub redirects data bearer creation directly to private MNO PGW.
- F **Roaming Hub:** Authoritative NS must be registered with GSMA Root DNS.
- G **Private EPC:** Roaming interfaces for S6a and S8 may be required in the private MNO for hybrid models.
- H **Private EPC:** S8HR IMS services require the private core must have its own IMS core.
- I **Public MNO MME:** APN-OI Replacement may not be universally supported in public MNO MMEs.
- J **IPX/Direct Interconnection:** The Roaming Hub provider must use Public, non-Internet routable IPv4 addresses as well as a unique ASN for BGP peering and interconnection.
- K **Private MNO and/or Roaming Hub Firewall:** The private MNO and/or Roaming Hub provider would need to configure and maintain firewall rules for the connected Public MNO(s) backbone IP ranges and associated ports for DNS, Diameter and GTP traffic.

Outbound Roaming – Hub

L **Numbering:** A private network offering IMS services would need to obtain telephone numbers from the appropriate numbering authority.

M **IMS Interworking:** IMS services are more susceptible to latency, jitter, and packet delay therefore, the interconnection model and bandwidth may need to be more robust than hosting other types of data applications. IMS Core would need to interwork with LEC/LD providers.

N **Private MNO UE:** For IMS to be supported, the private MNO UE could need a custom SHNI or SHNI+IBN SIP client.

10 Outbound Roaming – Local Breakout

Outbound roaming using the LBO model is the least popular method of deploying roaming services globally. LBO drastically changes how roaming functions across networks and relinquishes the control of data services from the HPLMN. LBO is well defined in [9] and [17] for an LTE system despite its lack of global popularity. Contrasting to a HR or Roaming Hub type of model this means subscribers receive access to local content instead of their home country/carrier content. At one point, LBO was speculated as a requirement to provide a VoLTE Roaming service given the additional latency that HR models cause but that has long since been disproven and LBO is now considered as obsolete within GSMA [34]. Figure 11 at the conclusion of this section depicts where key challenges exist as a visual reference to the LBO architecture model.

To provide an LBO service, from a public MNO standpoint, the MME permissions to allow inbound roaming are like other models, meaning it is common to configure permissions at a IMSI number series level, implying the MCC/MNC combination only. However, there could be additional nuances to ensure the QoS mapping is in alignment with the HPLMN as well as mapping of APNs to the HPLMN APN-OI for every SHNI. Similar to other models, MME configuration that extends to incorporate the SHNI 4-digit IBN (MCC+MNC+IBN) could drastically increase the table size as well as may not be configurable in all MME vendor software variants. Verification of MME capabilities requires discussion between a private and public MNO and should be understood as a non-standard configuration, thus, support and acceptance of this as a standard approach to uniquely permit a SHNI MCC/MNC+IBN as a IMSI number series is a potential issue. Additional configuration within a PGW is also necessary to support the specific APNs in the LBO agreement if they differ from the APNs provided within the VPLMN.

From a private network standpoint in the outbound roaming direction of a private network subscriber roaming on a public MNO, this method moves the data session anchor point from the HPLMN PGW to the VPLMN PGW. There is a defined interface (S9) for Visited PCRF (V-PCRF) to Home PCRF (H-PCRF), but this also implies that interface would need to be supported by the private and public MNOs, as well as introduces a coordination challenge to ensure that QoS profile values are aligned. This model maintains the S6a interface requirement which is similar to a HR or Roaming Hub type of model as the HSS remains in the private MNO and must provide the authentication and subscribed services to the VPLMN MME. At a subscriber level, the specific APNs allowed for LBO must be indicated by the HSS. For this architecture model it is required that the private EPC support the previously mentioned roaming interfaces. The continuing sub-sections assume the roaming interfaces are supported in the private EPC.

10.1 Diameter Signaling

Diameter signaling for an EPS leverages the existing Diameter Base Protocol as defined in [27] and incorporates specific requirements for the S6a (MME ⇔ HSS) interface in [28]. Of key importance for signaling on the S6a interface in the outbound roaming direction is routing of a Diameter command code with the request flag set, such as Authentication Information (318), or Update Location (316) to the appropriate destination network based on a realm using the format epc.mncXXX.mcc.YYY.3gppnetwork.org as defined in [29]. Diameter routing within a public MNO and between interconnection points is facilitated through one or more DA that maintain a SCTP association between each DA and eventually to EPC network elements such as an MME and HSS.

Commonly in a public MNO, there is a regional hierarchy of multiple DAs throughout the network for transmission of Diameter messages. While presumably common in a private network deployment, it would be uncommon for an MME in a large public MNO environment to associate directly to one or more HSS network elements. At the edge of a public MNOs network a DA would facilitate the connection to external networks,

commonly an IPX, or directly connected partner, and this network element is referred to as a DEA. Fundamentally, the functions and connection methods from a DEA are the same as a DA but would contain more specific route tables defined for destination-realms that exist externally from the public MNO. One of the fundamental key issues outlined in [30] indicates that the Destination-Realm AVP using the format defined in [29] constructed solely from the SHNI cannot uniquely identify the exact home network without additional unique identification at a subscriber level.

The following sub-sections focus on the Authentication Information and Update Location command codes primarily. Additional Diameter command codes for the S6a interface related to an MME and HSS, such as Cancel Location (317) and Insert Subscriber Data (319) are documented in [28]. Diameter command codes for other interfaces in the EPS such as Credit Control Request (CCR) and Credit Control Answer (CCA) for the S9 interface are briefly included as well. All other Diameter command codes are outside the scope of this section.

10.1.1 Authentication

The Diameter command code for Authentication Information as defined in [28] facilitates the exchange of subscriber authentication vectors to be used over the S1 interface between an MME and UE during the initial attach or TAU procedure(s) defined in [26] as well as for periodic re-authentication procedures as needed. The routing of this command code is based on the Destination-Realm AVP using the format defined in [29] and as previously indicated, the Destination-Realm AVP constructed solely from the SHNI cannot uniquely identify the private network. However, the unique subscriber identifier within an AIR message is borrowed from [27] as the User-Name AVP and is a logical identifier that could be used for customizing the Destination-Realm at a DEA network element. This would require direct agreement between a private and public MNO and should be understood as a non-standard configuration, thus, support and acceptance of this as a standard approach to uniquely identify a SHNI destination network is a Public MNO choice.

Alternatively, the HSS FQDN could be leveraged as the destination-host to route Diameter signaling but the HSS FQDN is not known by an MME until after a successful AIA is returned from an HSS which would include the origin-host AVP. As well, this HSS FQDN as a destination host is considered as optional in request messages and therefore is most likely ignored from a DEA route-table ruleset.

10.1.2 Update Location

The Diameter command code for Update Location as defined in [28] facilitates the validation of roaming permission and the exchange of subscribed services allowed for use in a VPLMN. A benefit of using a LBO architecture for the roaming model means that a private MNO as a HPLMN can control on a per subscriber basis whether roaming in a VPLMN is allowed, and further, which services, including APNs with associated QoS profiles, are allowed for LBO service. The specific AVPs contained in a ULR are well defined within [28] and the HSS learns the MCC/MNC of the VPLMN that originated the ULR based on the VPLMN ID AVP, following the format described in [28]. Of special note for LBO services, the HSS must indicate at the specific APN level whether it is allowed for LBO. This is controlled by setting the VPLMN-Dynamic-Address-Allowed AVP (code 1432) to 1, indicating allowed, or the default 0 indicating not allowed.

The routing of Diameter ULR messages and associated key issues for handling SHNI are the same as described for the Authentication Information procedures.

10.1.3 Credit Control

The CCR and CCA procedures are common Diameter messages between the Policy and Control Enforcement Function (PCEF) within a PGW and the PCRF within the PCC sub-architecture of an EPS. Other network elements within a PCC are out of scope for this section and thus the focus is specifically on the S9 interface as this is the logical connection between a V-PCRF and H-PCRF for an LBO model as defined in [35].

During visited access the V-PCRF and H-PCRF must communicate to negotiate QoS rules, this process is defined in [35] but it should be noted that the V-PCRF must perform QoS rule validation, implying that during a failure scenario a negotiation of rules between visited and H-PCRF occurs to apply the PCC rules to the visited PCEF. This also implies that through pre-configuration between private and public MNOs the QoS rules and application during visited access must be agreed upon. The interface between PCEF and PCRF within the visited network is defined as Gx and documented in [36]. For LBO, the same procedures as utilized within the visited network for home services for PCC rule provisioning apply.

Additional details on the S9 interface for LBO are defined in [35], notably though, [35] indicates a SCTP association must be in use for the S9 interface. Therefore, more investigation or discussion directly between a private MNO and public MNO may need to occur to determine if that is a direct SCTP association between V-PCRF and H-PCRF, or if the interface can leverage the existing SCTP association between PCRF's in either network and internal DA and DEA network elements. Finally, similar challenges as previously documented for routing of diameter messages using the Destination-Realm AVP may apply.

10.2 Access Point Name Resolution for Local Breakout PDN Connections

APN resolution is a fundamental process for determining the PGW during initial attach procedures, as well as during subsequent stand-alone PDN Connection Request procedures for UEs that require multiple data bearers. The APN resolution process within an EPS follows the well-defined NAPTR process defined in RFC 3403 and by 3GPP in [31], specifically using the S-NAPTR procedure. The S-NAPTR process allows for the authoritative NS to provide a list of PGW candidates which can later be queried for their respective A record (IPv4) as described in [31]. With LBO, topology mapping is leveraged to keep the SGW and PGW functions as close to the UE as possible. However, the nuances of APN resolution as it relates to topology mapping is considered out of scope for this section.

The intent of this section is to focus on the APN resolution process as it relates to SHNI in an LBO environment with some foundational background on APN structure and resolution procedures. It is important to be familiar with the ESM procedures described in [26] for how a UE requests creation of a data bearer, as well as how an MME performs any necessary subscription validation of the requested bearer. Also, of note, is the VPLMN-Dynamic-Address-Allowed AVP that is optionally included in the Diameter ULA or IDR which if supported in the HSS and MME allows the APN-OI portion of an APN to match the VPLMN.

10.2.1 APN Structure

As defined in [29] an APN is comprised of both an APN-NI and APN-OI through concatenation of a string of labels to form a FQDN. The APN-NI portion is commonly referred to simply as an APN but specifically represents the alphanumeric contents, potentially containing multiple labels, that are configured in the HPLMN HSS and PGW network elements as well as other necessary systems for data bearer management such as a PCRF. The APN-NI is also commonly configured within a UE although there are methods for the HSS to

provide a default APN for data bearer creation and the UE could optionally not send the requested APN to the MME during the EMM and ESM procedures defined in [26]. There are additional rules related to maximum length and disallowed character strings further defined in [29].

The APN-OI portion is constructed by an MME based on the MCC/MNC of the requesting IMSI, or in the case of LBO based on MME configuration for the LBO supporting APN. The standard format for each concatenated label in the APN-OI is defined in [29] and takes the form of "mncXXX.mccXXX.3gppnetwork.org" where XXX are the values 0-9 from the MCC/MNC. In the case of a 2-digit MNC a leading 0 is always inserted. As well, the labels "apn.epc" are inserted between the APN-NI and APN-OI to form the APN FQDN as indicated in [29].

The APN-NI presents a challenge for a private MNO when attempting to use the LBO model for roaming on a public MNO due to the lack of widespread commercial usage of LBO in public MNO networks. The APN-NI portion is primarily meaningful within the private MNO when no roaming is in use and thus could be anything the private MNO desired but with an LBO model the APN-NI must be unique within the Public MNO networks as well as any other private MNO that also could use an LBO model with the same public MNO. This is because, ultimately, the entire APN FQDN must be unique and resolve only to a specific PGW(s), which now would include the public MNO network. The APN-NI challenges can be overcome by each private MNO including a label that aligns to their IBN in the APN-NI portion and use that same APN in their private EPC as well as when attempting to use a VPLMN.

10.2.2 HSS Parameters for LBO

The VPLMN-Dynamic-Address-Allowed AVP as defined in [28] is controlled by an HSS to indicate on a per APN basis whether that APN is allowed to use the HPLMN PGW or the VPLMN PGW. The default setting for this AVP is "NOTALLOWED" which has the same meaning if not present in the ULA. VPLMN-Dynamic-Address-Allowed AVP is nested within the Subscription-Data, APN-Configuration-Profile and eventually the APN-Configuration AVPs and is applicable only for the specific APN defined in the Service-Selection AVP of that APN-Configuration profile. Therefore, its inclusion as allowed is unique only to the specified APN and other APNs could leverage a HR or even a Roaming Hub model.

10.2.3 IP Routing and Firewall Permissions

As recommended in [23] both MNOs and IPX providers should perform traffic filtering at their network edge. Within the public MNO space, this means that any RFC 1918 private addresses should be blocked as well as specific rule functionality to prevent source IP address spoofing needs to be accounted for [23]. However, unlike the HR and Roaming Hub architecture models, there is minimal impact for IP Routing and Firewall permissions in an LBO architecture as the primary interfaces in use are S6a and S9 which are Diameter based. Depending on the requirements for SCTP association between V-PCRF and H-PCRF as defined in [36] there could be a need for IP routing directly between these network elements, which may differ from a S6a interface connection introducing potential impacts related to the exchange of IP routing data like what would normally be included in an IR.21.

A more complicated model would include the private MNO also maintaining an IPX connection, or at minimum a direct connection for customization of certain APNs that require HR or Roaming Hub provider connectivity. For simplicity this complex architecture model is outside the scope of this section but as needed refer to sections 8.2.3 or 9.2.4 for HR or Roaming Hub models respectively.

10.3 IMS

IMS refers to an additional core network that enables the ability for voice, SMS, and video to use an IP based network as a replacement for circuit switched service. Commonly, IMS and VoLTE or ViLTE are used synonymously but it is important to understand the distinction that VoLTE, ViLTE and SMS over IMS are services provided by an IMS core network as opposed to being a network themselves. IMS utilizes the well-established SIP and RTP, among other protocols, for the exchange of datagrams between a client and server inside a MNOs network. The same protocols are also used in other common VoIP applications.

From a services standpoint, IMS enables the ability for a UE to use VoLTE, ViLTE, and SMS over IMS regardless of location, and in the roaming case, the HR model is the most common. If a private MNO desires to have IMS services available inside the private EPS, this insinuates either the private MNO EPS includes a separate IMS core, or they have agreed with a 3rd party to host an IMS core. Because the LBO model allows for each APN to be separately managed it is possible for IMS to use a different roaming model, such as HR or a Roaming Hub, while other APNs are allowed for LBO. If a HR or Roaming Hub model are chosen for IMS it assumes the S8 interface is supported in the private MNO as well as then requires establishment of an interconnection method, IP route advertisement exchange, firewall management, and APN resolution.

The LBO model was once believed to be required for IMS to be used in a roaming environment due to latency impacts, but that approach has long since been considered obsolete [34]. IMS is additionally complicated in an LBO model as this could imply a private MNO does not have an IMS core of their own as well as may not intend to leverage IMS based functions inside the private EPS. Voice based services should be continuous inside and outside of a UE's home network in order to provide the best user experience and leveraging IMS only when roaming using LBO means the same service, using the same MSISDN, would not be provided in the HPLMN. If a private MNO does have an IMS core and desired for a seamless experience leveraging LBO when roaming for IMS, this would introduce an additional interconnection requirement between both the private and public MNOs IMS platforms.

Regardless of the roaming model chosen for a private MNO there is still a requirement to obtain telephone numbers from the appropriate numbering authority, such as the NANPA in addition to interconnecting to one or more LEC and LD carriers. Additionally, the UE requirements for IMS services, which include a SIP client using the appropriate parameters for the home MNO, or hosted IMS solution also represent a challenge given a wide range of device manufacturers. Further UE requirements for IMS are defined further in [32].

10.3.1 Well-known IMS APN

Within the public MNO environment, it is understood and accepted that IMS services use the well-known APN of "IMS" [32]. This allows for QoS policy mapping to the appropriate QCI during session creation for the Non-GBR bearer. Within [33], 3GPP indicates the non-GBR bearer for IMS Signaling is QCI 5, which also has one of the highest priority values, and therefore utilizing a standardized APN allows for more consistent alignment of QCI assignment between a MME, HSS and PCRF inside of a MNOs network as well as during roaming scenarios.

The well-known IMS APN presents a challenge for SHNI based networks as the APN-NI portion cannot be used explicitly to identify a private network. Recall that the APN-OI portion has a fixed length for MCC/MNC digits as well, which preclude any possibly of manipulation to uniquely identify an SHNI entity by IBN. As well, the APN-NI portion offers the ability to append a label that uniquely identifies the SHNI entity and can be manipulated through HSS assignment or through APN-OI replacement. However, if this approach is used for the IMS APN, it would require direct agreement between a private and public MNO to support this new custom IMS APN variant. Therefore, it should be understood as a non-standard configuration. Support and acceptance of this as

a standard approach to map a custom IMS APN to QCI 5 is a Public MNO choice. Some device manufacturers may also only support the well-known IMS APN and may require direct involvement to further understand if any non-standard customer IMS APN can be supported.

10.3.2 OTT

An alternative to EPS provided IMS services for a private network includes the use of commercially available or enterprise OTT applications. An OTT solution for real-time exchange of VoIP allows for flexibility and simplicity if a private network does not have the ability or desire to maintain a dedicated IMS core.

10.4 Key Issues for Outbound Roaming with Local Breakout

The use of LBO is an alternative architecture model to HR and Roaming Hub and while mitigating some challenges it can introduce additional complexities for both a private and a public MNO. While some of the key issues are reconcilable through direct agreement for non-standard handling, others require further evaluation. The architecture of a local breakout solution is shown in the following figure, with the labelled items briefly discussed in the following list.

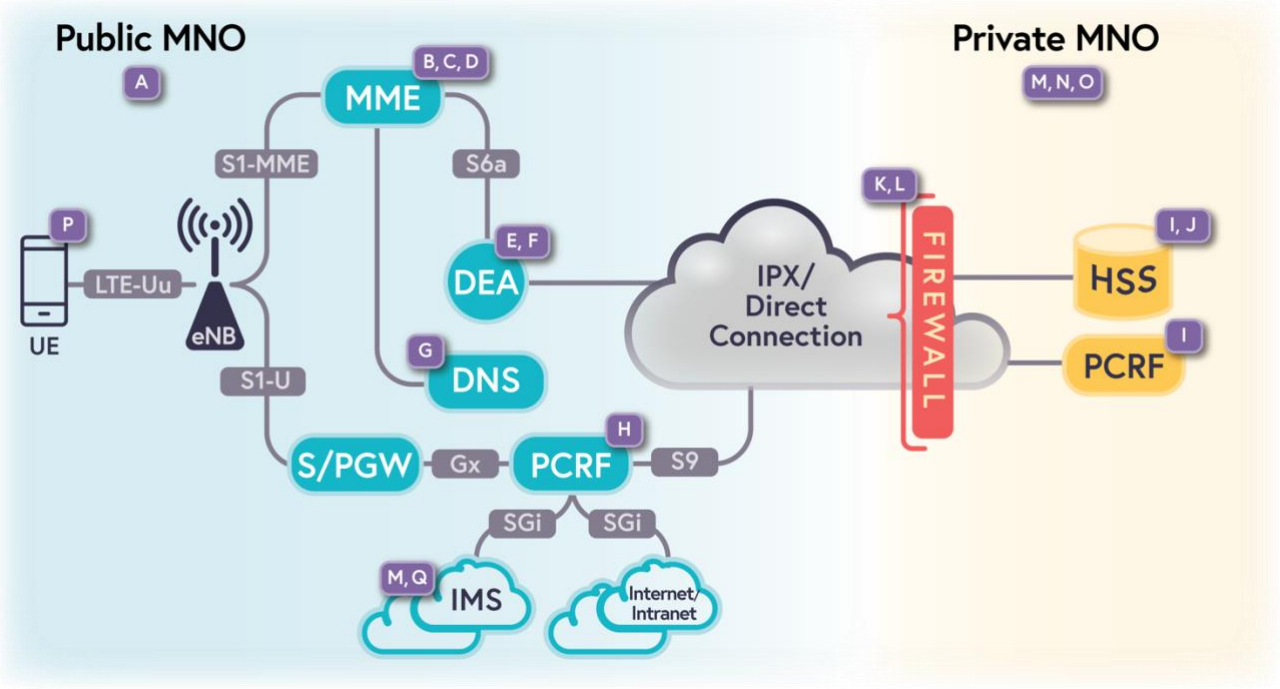

Figure 11: Key Issues for Outbound Roaming – Local Breakout

Throughout this section the following key issues (not listed in priority order) shown in the above diagram have been raised for awareness purposes only:

- A **Architecture Model:** LBO usage globally is unpopular and is considered as obsolete by GSMA.
- B **Public MNO MME:** MME permissions may not be configurable beyond 5 or 6 digits to incorporate the SHNI MCC/MNC+IBN combination.

Outbound Roaming – Local Breakout

C **Public MNO MME:** Configuring LBO at an entire MCC/MNC level for a SHNI prevents other models from being leveraged.

D **Public MNO MME:** The VPLMN-Dynamic-Address-Allowed AVP must be supported by the MME.

E **Public MNO Diameter:** There is no SHNI indicator in the destination realm for Diameter routing.

F **Public MNO Diameter:** User-Name AVP routing is non-standard.

G **Public MNO EPC:** APN-NIs for a private MNO must be configured within the home authoritative DNS and PGW and cannot overlap with any of the VPLMN home customers.

H **Public MNO PCC:** QoS rules and policy must be negotiated and possibly configured in a custom manner for each SHNI.

I **Private EPC:** Roaming interfaces for S6a and S9 must be supported in the Private EPC.

J **Private MNO HSS:** The VPLMN-Dynamic-Address-Allowed AVP must be supported by the HSS.

K **IPX/Direct Interconnection:** The private MNO must interconnect directly or through an IPX for Diameter SCTP based connections.

L **Private MNO Firewall:** The private MNO would need to configure and maintain firewall rules for the connected Public MNO(s) backbone IP ranges and associated ports for Diameter.

M **IMS Interworking:** IMS services offered as LBO within the VPLMN would not work while in the Private MNO, creating an inconsistent customer experience.

N **IMS Interworking:** A private network offering IMS services as HR or through a Roaming Hub while leveraging LBO for other APN's would still need to maintain an S8 connection with public non-routable IP addresses as well as the IMS Core would need to interwork with LEC/LD providers.

O **Numbering:** A private network offering IMS services as HR while leveraging LBO for other APN's would need to obtain telephone numbers from the appropriate numbering authority.

P **Private MNO UE:** For IMS to be supported, the private MNO UE could need a custom SHNI or SHNI+IBN SIP client.

Q **IMS APN:** The IMS APN is standard, therefore conflicts between a Public MNO's home and private MNO subscribers could create complex configuration in a VPLMNs IMS Core.

11 Private-to-Private Roaming

Private networks may have a unique need to leverage services among multiple locations or campuses owned by the same enterprise, or through prior agreement, with another enterprise. In this case, services from each private network island could constitute roaming using one of the many models detailed in prior sections, such as Home Routed, Roaming Hub, or Local Breakout. In this manner, there would still be a Home and Visited network, with the difference being that both networks are considered as private. Because both networks are private there should be a direct agreement between the two or more network entities, which could be the same or different enterprises.

Any of the previously mentioned roaming models could solve this problem but there are other alternatives as well given that the networks serving as Home or Visited are private, and therefore allow for non-standard avenues to providing service continuously across the private network locations. Based on the concept that roaming with private networks should not be treated like traditional roaming across public networks used today, the following sub-sections present a novel approach to addressing this use case, referred to as Collaborative Camping, which incorporates the following assumptions:

- Inter-private network transitions will be based on collaboration across the enterprises.
- Roaming indicator will not be turned on.
- Usage based metrics for cross charging will typically not apply.
- Routing for authentication from visited network to the home enterprise network may need to be simplified as the traditional interfaces like the S6a are typically not supported by private networks.
- Local breakout for data connectivity with the visited network avoiding all packets to be routed to the home enterprise network.
- Local breakout avoids costs of home routing and reduces end-to-end latency.

11.1 Collaborative Camping

The term Collaborative Camping suggests that an enterprise(s) is collocating the resources necessary to complete authentication procedures when a device is transitioning to another private network using a private network credential. In this method, the EUD transitions to another private network when out of the footprint of its enterprise network by using periodic scans or using the geofencing feature defined on TS-1004 [37]. The EUD may find a private network based on the agreements in place for EUD operations and the available networks in EUD's current location.

The authentication functions as part of the network registration procedures would need a mechanism to identify the HPLMN domain where the credential is stored. This inter-enterprise authentication is addressed by using a hierarchical HSS and can be treated as a home network when transitioning across enterprises along with SHNI-IBN based routing. The EUD operates on the visited network without the roaming flag turned on given that broadcast PLMN used to select the network is identified as the home or equivalent-home network but the SIM.

The data is offloaded as LBO traffic to access the Internet / Intranet and any home enterprise access is supported as VPN tunnels. When specialized traffic support is needed, explicit PDN connection to the home enterprise is established. However, this requires DNS support to find the PDN GW in the home enterprise network which could also involve establishing a dedicated connection between the private MNOs, similar to

the HR roaming model. Similar connectivity may need to be established for policy management functions. The key concepts and benefits of this alternative architecture model are:

- Routing for authentication from visited network to the home enterprise network.
- Local breakout for data connectivity with the visited network avoiding all packets to be routed to the home enterprise network.
- Reduced or eliminated costs related to home routing.
- Reduced end-to-end latency.
- Allows connectivity for specific PDN / DN that require home routing. Used as an exception when needed.

11.2 Architecture for Collaborative Camping

Figure 12 provides a high-level view of the visited network and home enterprise network architecture for connectivity.

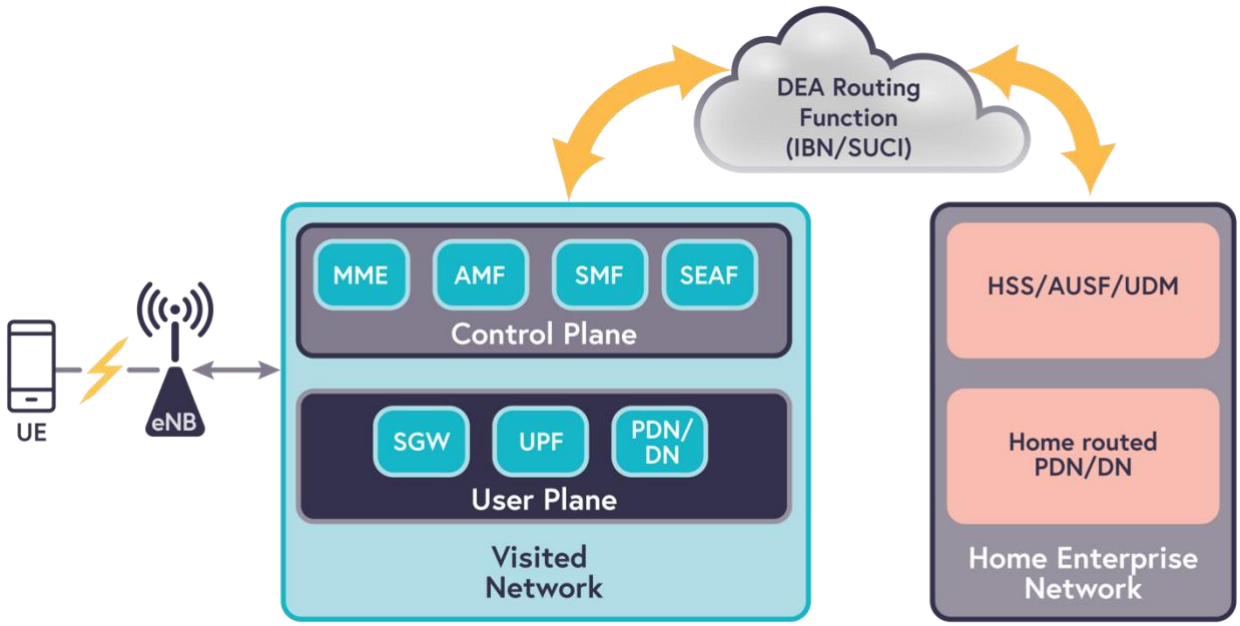

Figure 12: Collaborative Camping Architecture

11.3 Key Issues for Collaborative Camping

Private-to-Private roaming shares many common key issues already discussed but most notably for this roaming direction is handling of Diameter routing from a serving MME to a home HSS as well as PGW identification to support local breakout.

- **Hierarchical HSS:** Commonly, an HSS is single network element, and a hierarchical structure implies an HSS includes Diameter proxy capabilities which would more commonly exist as a Diameter function prior to signaling reaching an HSS.
- **Symmetric Diameter Routing:** Diameter routing is symmetric, implying that a hierarchical HSS capability would mean that the first HSS in the path would insert its host name as in the Route-Record AVP and

would therefore also need to process an Answer message, thus increasing load for handling of Diameter messages.

- **Architecture Model:** LBO usage globally is unpopular and is considered as obsolete by GSMA.
- **Private MNO MME:** MME permissions may not be configurable beyond 5 or 6 digits to incorporate the SHNI MCC/MNC+IBN combination.
- **Private MNO MME:** Configuring LBO at an entire MCC/MNC level for a SHNI prevents other models from being leveraged.
- **Private MNO MME:** The VPLMN-Dynamic-Address-Allowed AVP must be supported by the MME.
- **Private MNO EPC:** APN-NIs for a private MNO must be configured within the home authoritative DNS and PGW and cannot overlap with any of the VPLMN home customers.
- **Private MNO PCC:** QoS rules and policy must be negotiated and possibly configured in a custom manner for each SHNI.
- **Private EPC:** Roaming interfaces for S6a must be supported in the Private EPC.
- **IPX/Direct Interconnection:** The private MNOs must interconnect directly or through an IPX for Diameter SCTP based connections.

12 Inbound Roaming

Inbound roaming refers most closely to the use case presented in section 7.2, Public-to-Private network roaming. As mentioned in section 7.2, a leading architecture model for this roaming direction could be MOCN, however, this section intends to explore how inbound roaming could function with a more traditional roaming model. For simplicity, only the well-defined HR model will be reviewed. Figure 13 at the conclusion of this section depicts where key challenges exist as a visual reference to the HR architecture model for Inbound roaming.

The benefits of a HR roaming model as discussed in relationship to Private-to-Public roaming are the same, specifically, a HR model allows the home MNO to maintain control at an individual subscriber level for which services are available to that subscriber during roaming. Under normal roaming circumstances this also implies the home MNO can control at a VPLMN level which serving networks are allowed for roaming.

Devices from a public MNO would need to support the CBRS frequency bands, band 48 for LTE and N48 for 5G Standalone (5G SA) in order to receive the network broadcast when performing a PLMN scan. Many newer devices, e.g., smartphones, may already support these bands, but this is potentially MNO dependent, as the carrier build OS will ultimately determine which bands are enabled when a commercial MNO SIM is interested to the device. Further discussion on how commercial MNOs determine and device manufacturers determine band availability is outside the scope of this paper.

12.1 Network Broadcast

Whether the RAN is a public or private MNO, there always needs to be a network broadcast consisting of a MCC and MNC, among other network specific parameters. For a private enterprise the network broadcast would be the SHNI MCC/MNC of 315/010 on a CBRS frequency in accordance with [24]. The MCC/MNC of the broadcasting network traditionally implied uniqueness as each public MNO was assigned a dedicated MCC/MNC from the appropriate regional management entity. For a private network, the SHNI is not unique, which therefore can create a significant challenge for a public MNO to control where roaming to a private network should be allowed. Specifically, when the HR model is combined with the OnGo SHNI the home MNO is not able to tell the difference between private networks when the VPLMN ID is presented with the same MCC/MNC digits. However, if the significant work to interconnect a private and public network is not in place roaming would not be possible anyway. Finally, a significant challenge exists for public MNO devices due to the possibility that the public MNO broadcast, even if weak, could be available in the same area. If the UE is connected to its HPLMN broadcast, that will prevent the UE from performing a background scan to even be able to see the private network broadcast.

12.2 Controlling Access for Inbound Roaming

For an LTE network, MME permissions to allow inbound roaming are commonly configured at a IMSI number series level, implying the MCC/MNC combination only. For a private MNO providing inbound roaming, this granularity allows for the same level of control a public MNO would have, presuming the inbound roaming subscribers have a dedicated MCC/MNC from their public MNO. There are numerous other interconnection configurations necessary to support inbound roaming, but the MME provides the first line of access control. The private network EPC must support the roaming interfaces in addition to being compliant with 3GPP standards, notably for handling network rejections [26] among others. This is critically important with a SHNI broadcast as a public MNO may choose to roam on one private network but not another, marking the SHNI as forbidden on a public MNO SIM could cause service impacts for the public MNO device in other SHNI roaming

areas that were intended to be allowed. Additionally. The private MNO would need to ensure there is enough RAN and EPC capacity to handle public MNO traffic, which could have negative implications for resource availability of the private MNO devices.

12.3 Interconnection

Section 4 discusses general interconnection details, including options to connect via an IPX as well as through a direct connection. Inbound roaming on a SHNI private MNO seems more applicable with the traditional IPX connection model unless the private MNO only intended to connect to one public MNO network. With an IPX connection the private MNO would need to allow the public MNO IMSI number series within the MME, as well as configure the necessary connection for APN resolution, Diameter, and S8 for GTP traffic. Each protocol layer for inbound roaming to function comes with its own set of configuration challenges. Following is a brief list of configuration challenges for DNS, Diameter, and GTP.

For DNS, the private MNO serving inbound roaming subscribers from Public MNOs would need to either locally maintain zones files on its DNS to point public MNO APN-OI's to the respective DNS hostnames and IP addresses of the public MNO authoritative DNS. Alternatively, the private MNO could leverage the root DNS service provided by an IPX described in section 4.1.3.

For Diameter, the private MNO would need to establish an SCTP association to an IPX DEA and point the public MNO destination realm(s) to the connected DEA. As well, the origin-realm of the private MNO would need to include a custom label in addition to the standard realm of epc.mnc010.mcc315.3gppnetwork.org, otherwise, the public MNO could not uniquely identify the specific private MNO for return routing of Diameter messages.

For GTP, the private MNO would need to maintain routing table entries to each public MNO backbone IP range, as well as ensure sustainment processes exist to account for when public MNOs add new IP ranges to their network. Traditionally, the routing table entries are injected through BGP neighbor route advertisements as well as a GSMA defined procedure for exchanging IR.21 details that include all backbone IP ranges. Finally, a private MNO would need to maintain firewall configuration for the previously mentioned protocols, DNS, Diameter, and GTP.

12.4 Key Issues for Inbound Roaming

Private-to-Public roaming follows the more traditional HR architecture model used commonly by public MNOs that wish to roam unilaterally or bilaterally with other public MNOs. The architecture of an inbound roaming solution is shown in the following figure, with the labelled items briefly discussed in the following list.

Private-to-Private Roaming

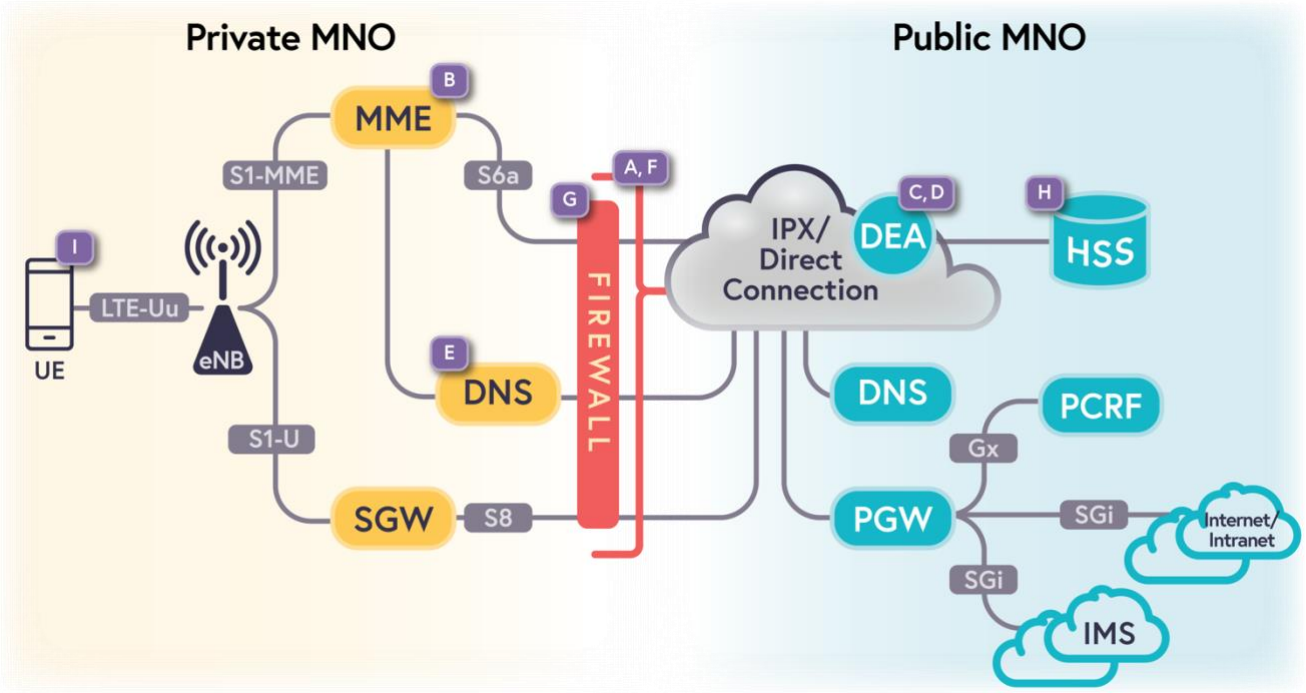

Figure 13: Key Issues for Inbound Roaming

Throughout this section the following key issues (not listed in priority order) have been raised for awareness purposes only:

- A **Private EPC:** Roaming interfaces for S6a and S8 must be supported in the Private EPC
- B **Private MNO MME:** MME permissions would include the common 5- or 6-digit public MNO IMSI Number Series.
- C **Private MNO Diameter:** The private MNO would need a customized origin-realm for Diameter routing as well as maintain an SCTP association either to an IPX DEA or directly to a public MNO DEA.
- D **Public MNO Diameter:** Required to maintain diameter route rules for the customized origin-realm of the private MNO(s) for Diameter routing.
- E **Private MNO DNS:** Locally manage zone files for the public MNO APN-OI to authoritative hostname or leverage the IPX root DNS lookup procedure.
- F **IPX/Direct Interconnection:** The private MNO must use Public, non-Internet routable IPv4 addresses as well as a unique ASN for BGP peering and interconnection.
- G **Private MNO Firewall:** The private MNO would need to configure and maintain firewall rules for the connected Public MNO(s) backbone IP ranges and associated ports for DNS, Diameter and GTP traffic.
- H **Public MNO HSS:** The public MNO would be unable to differentiate the VPLMN ID of the private MNO when each is using the SHNI for network broadcast.
- I **Public MNO UE:** A UE that is connected to its HPLMN broadcast will remain camped on the HPLMN even when in range of the private MNO broadcast.

13 MOCN RAN Sharing

MOCN refers to Multi Operator Core Network. it is an LTE Network feature that allows multiple Operators and Service Providers to share RAN systems or CBSDs. The scope of this feature falls outside Roaming whitepaper. Future working guides shall focus on MOCN RAN sharing processes. The OnGo requirements for MOCN are provided in [25] and [38]. A general brief shall be described below.

In a MOCN Neutral Host Network (NHN), the eNB is shared between Participating Service Provider (PSP)s, with the shared eNB routing traffic of a given UE to the appropriate PSP. From the user's perspective, the connection appears to come from their home network, transitioning seamlessly to and from the network. The NHN can only support up to six PSPs per channel in LTE, but the PSPs don’t have to provide dedicated equipment to support the system.

MOCN functionality is typically integrated into the eNB as a feature. If the eNBs do not support MOCN directly, a MOCN gateway system can be used to provide the needed MOCN interfaces. A MOCN gateway can also be used to aggregate the interfaces of multiple eNBs, providing a single connection point to the PSPs’ networks. Individual gateways for each PSP can be used, which allows the gateways to be configured and maintained individually, increasing overall reliability.

A MOCN architecture is preferred when there are a large number of CBSDs. Having different channels for each PSP, as required for Multiple Operator Radio Access Network (MORAN) would result in too many channels. A MOCN gateway is included in the system design, to consolidate the connections to the CBSDs.

The MOCN architecture illustrated in Figure 14 below for CBRS MOCN for Neutral Hosting is the 3GPP EPS system architecture as specified in 3GPP TS23.401 [17] and associated specifications. It is assumed that RAN sharing is in use between multiple EPCs as specified in 3GPP TS 23.251 [39]. Each EPC is associated with a PLMN ID. UEs use the Shared CBRS RAN for connecting to their selected PLMN. For CBRS spectrum management, interaction between the Shared CBRS RAN and SAS is assumed by the NHN provider.

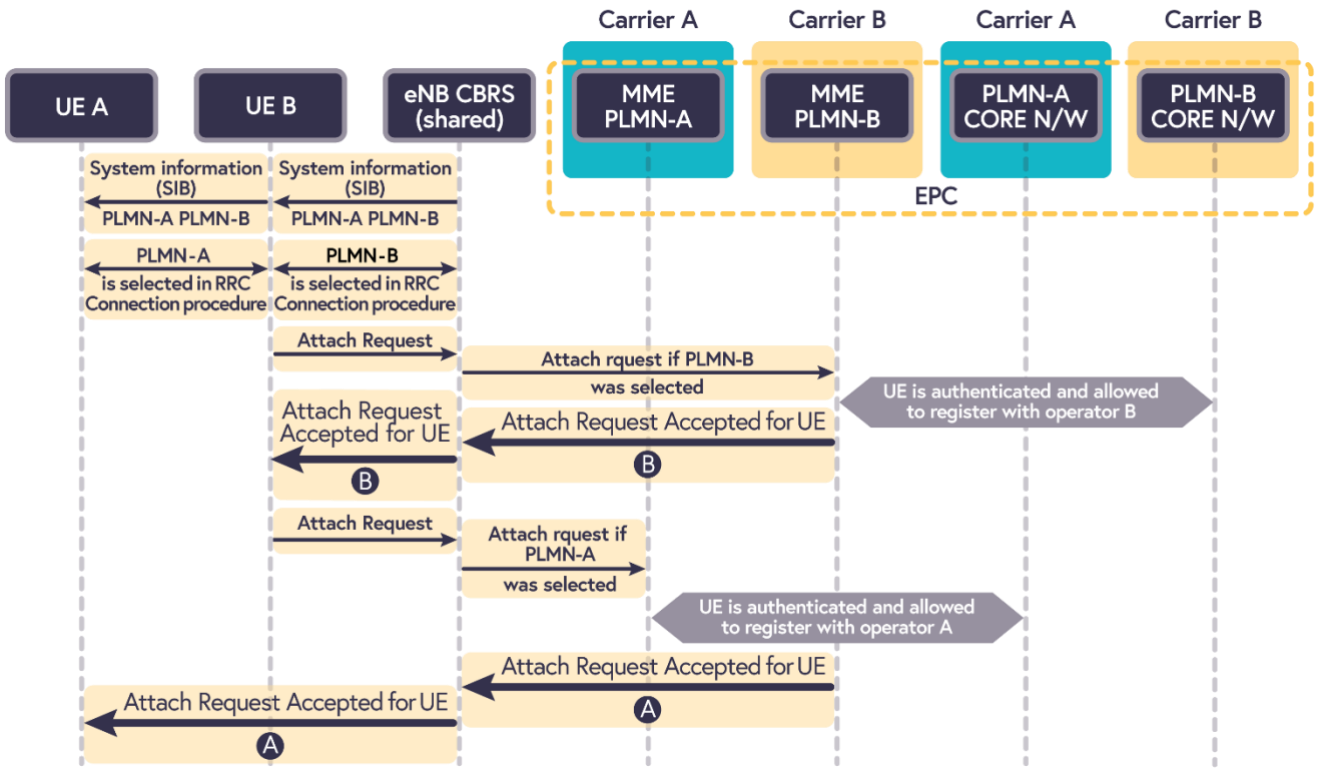

Figure 14: MOCN Architecture

The use of MOCN requires a service SLA between the neutral host provider managing the CBSD and the hosted core network clients. This SLA defines the QoS policy aspects as well as making technical provisions for connection of the neutral host's eNB to the client core network via the S1 interface. To ensure successful deployment both parties work on technical integration and interoperation. The MOCN neutral host requires access to certain hosted client-specific information such as the ability to connect and communicate with the appropriate list of adjacent cells for each hosted client core. Network security aspects will need to be addressed.

The radio interface for a MOCN solution will typically operate in CBRS spectrum managed by the Neutral Host. To ensure good Spectrum coexistence, SAS relations managed by one entity is best. The MOCN standard does not specify how spectrum is divided between hosted Carriers. It is up to the neutral host to agree upon a policy with their Carriers for the spectrum resources to be used.

Prioritization and management of traffic on the radio interface is not standardized in MOCN. The eNB is responsible for enforcement of policy which must be agreed between the neutral host and each Carrier. Options such as fixed resource reservations for each carrier or completely shared resources for all Carriers, or combined approaches that support a mixture of reserved and shared resources can be decided on based on SLAs.

Mobility topics shall be described in more detail in future guides.

14 Deployment Options

The use cases discussed in this paper present multiple different deployment options, some of which may contradict, or limit the ability to use other roaming models. This is true especially for LBO, whereas if LBO is selected as the roaming architecture model the same VPLMN cannot also support a Home Routed model for the same SHNI MCC/MNC. The following sub-sections show a more detailed view of call flows related to Initial Attach procedures for each roaming model previously discussed.

14.1 Home Routed via IPX

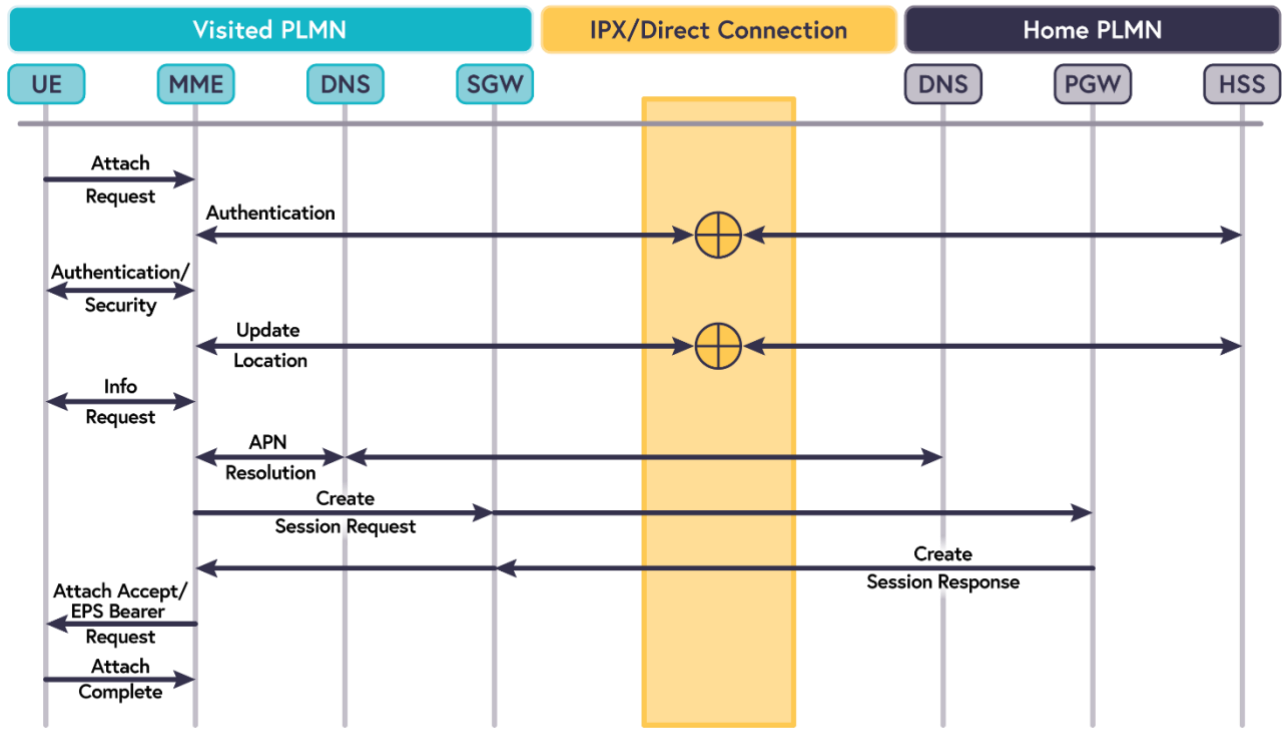

Figure 15: CBRS Registration and S8 Home Routed Call Flow

1. **EMM Attach Request and ESM PDN Connectivity Request:** Non-Access-Stratum (NAS) Operation sent in the direction of UE to MME (via eNB). The ESM PDN Connectivity Request message is combined with the EMM Attach Request message. The EPS Mobile Identity will be included within the message as either the IMSI or Globally Unique Temporary ID (GUTI). If the GUTI is used, and not known by the MME, the MME would initiate an EMM Identity Request procedure to obtain the IMSI of the UE (not shown).
2. **Authentication Information Request/Answer (AIR/AIA):** DIAMETER operation initiated by an MME to HSS to request unique authentication vectors from the HSS.
3. **EMM Authentication Request:** NAS Operation sent in the direction of MME to UE (via eNB). The EMM Authentication Request message is used to challenge the UE with the authentication vector provided by the HSS. Authentication is mutual and the UE will ensure the network originating the Authentication Request message is valid.

4. **EMM Authentication Response:** NAS Operation sent in the direction of UE to MME (via eNB). The EMM Authentication Response message is used to provide the RES after the UE has completed processing the Authentication Request. The MME will check the RES with the XRES provided by the HSS.
5. **EMM Security Mode Command:** NAS Operation sent in the direction of MME to UE (via eNB).
6. **EMM Security Mode Complete:** NAS Operation sent in the direction of UE to MME (via eNB).
7. **ESM Information Request:** NAS Operation sent in the direction of MME to UE (via eNB). The ESM Information Request message is used to obtain the APN the UE wants to use in order to establish a Default EPS Bearer.
8. **ESM Information Response:** NAS Operation sent in the direction of UE to MME (via eNB). The ESM information Response message is used by the UE to provide the APN to be used for the Default EPS Bearer.
9. **Update Location Request/Answer (ULR/ULA):** DIAMETER operation initiated by an MME to HSS to notify HSS of a subscriber registration attempt and to request subscription data. The HSS will always return a ULA for a ULR which would include a Result Code of Diameter_Success and include the subscription data or one of the 3GPP 29.274 defined rejection codes.
10. **APN Resolution:** After an optional subscription check by an MME to ensure the requested APN is allowed by an HSS an MME will initiate a DNS procedure with the query type of NAPTR to identify the PGW Replacement names for the APN FQDN. A second A record query may be initiated if necessary to obtain the A record (IPv4 address) of the PGW replacement name.
11. **Create Session Request:** GTP Control Plane version 2 (GTP-Cv2) operation sent in the direction of MME to SGW and SGW to PGW. The Create Session Request is used to notify the PGW of the Bearer requested by the UE and to establish a signaling tunnel between MME and SGW as well as signaling and user-plane tunnel between SGW and PGW.
12. **Create Session Response:** GTP-Cv2 operation sent in the direction of PGW to SGW and SGW to MME. The Create Session Response is used to setup the S5/S8 Bearer (SGW ↔ PGW) and a signaling tunnel between SGW and MME.
13. **EMM Attach Accept and ESM Activate Default EPS Bearer Context Request:** NAS Operation sent in the direction of MME to UE. The ESM Activate Default Bearer Request message is used to provide the UE with an IP address for the requested APN as well as the assigned QoS parameters.
14. **EMM Attach Complete and ESM Activate Default EPS Bearer Context Accept:** NAS Operation sent in the direction of UE to MME. The combined EMM and ESM message is used by the UE to acknowledge completion of the Attach Request and Default EPS Bearer establishment. A Data Radio Bearer (DRB) is established between the UE and eNB.
15. **Modify Bearer Request:** GTP-Cv2 operation sent in the direction of MME to SGW. The Modify Bearer Request is used to notify the SGW that the DRB has been established and to provide the eNB Tunnel End Point ID (TEID) so the S1 User plane (S1-U) bearer can be established.
16. **Modify Bearer Response:** GTP-Cv2 operation sent in the direction of SGW to MME. The Modify Bearer Response is used to notify the eNB of the SGW S1-U TEID to setup the S1-U Bearer (SGW ↔ eNB).

Note: Modify Bearer Request/Response operations are used for many different purposes during the lifecycle of a data bearer, in some cases the procedures would be between MME and SGW only in the VPLMN and in others the Request message would be forwarded to the PGW in the HPLMN.

14.2 Home Routed via Hub

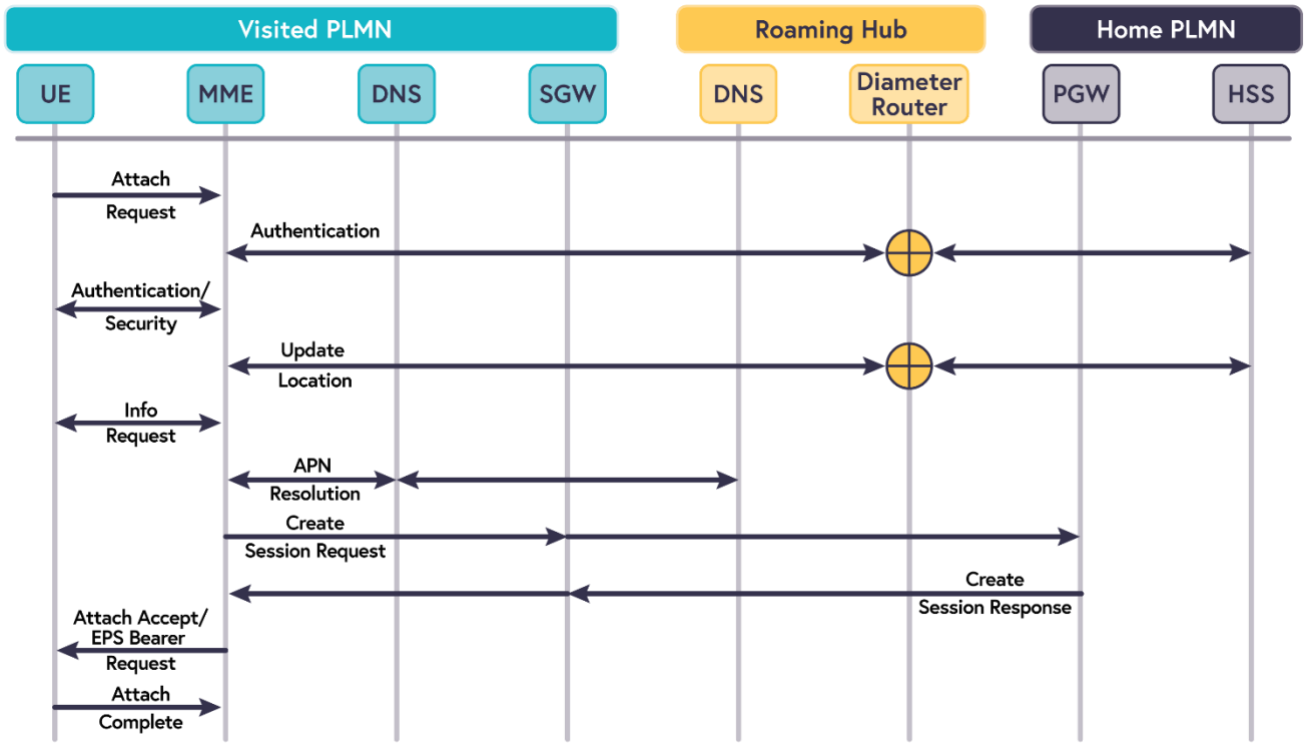

Figure 16: LTE Registration with Roaming Hub Call Flow

1. **EMM Attach Request and ESM PDN Connectivity Request:** NAS Operation sent in the direction of UE to MME (via eNB). The ESM PDN Connectivity Request message is combined with the EMM Attach Request message. The EPS Mobile Identity will be included within the message as either the IMSI or GUTI. If the GUTI is used, and not known by the MME, the MME would initiate an EMM Identity Request procedure to obtain the IMSI of the UE (not shown).
2. **Authentication Information Request/Answer (AIR/AIA):** DIAMETER operation initiated by an MME to HSS to request unique authentication vectors from the HSS. The Roaming hub provider would facilitate redirection of the AIR to the appropriate HPLMN HSS.
3. **EMM Authentication Request:** NAS Operation sent in the direction of MME to UE (via eNB). The EMM Authentication Request message is used to challenge the UE with the authentication vector provided by the HSS. Authentication is mutual and the UE will ensure the network originating the Authentication Request message is valid.
4. **EMM Authentication Response:** NAS Operation sent in the direction of UE to MME (via eNB). The EMM Authentication Response message is used to provide the RES after the UE has completed processing the Authentication Request. The MME will check the RES with the XRES provided by the HSS.
5. **EMM Security Mode Command:** NAS Operation sent in the direction of MME to UE (via eNB).
6. **EMM Security Mode Complete:** NAS Operation sent in the direction of UE to MME (via eNB).

7. **ESM Information Request:** NAS Operation sent in the direction of MME to UE (via eNB). The ESM Information Request message is used to obtain the APN the UE wants to use in order to establish a Default EPS Bearer.
8. **ESM Information Response:** NAS Operation sent in the direction of UE to MME (via eNB). The ESM information Response message is used by the UE to provide the APN to be used for the Default EPS Bearer.
9. **Update Location Request/Answer (ULR/ULA):** DIAMETER operation initiated by an MME to HSS to notify HSS of a subscriber registration attempt and to request subscription data. The Roaming hub provider would facilitate redirection of the ULR to the appropriate HPLMN HSS. The HSS will always return a ULA for a ULR which would include a Result Code of Diameter_Success and include the subscription data or one of the 3GPP 29.274 defined rejection codes.
10. **APN Resolution:** After an optional subscription check by an MME to ensure the requested APN is allowed by an HSS an MME will initiate a DNS procedure with the query type of NAPTR to identify the PGW Replacement names for the APN FQDN. A second A record query may be initiated if necessary to obtain the A record (IPv4 address) of the PGW replacement name.
11. **Create Session Request:** GTP-Cv2 operation sent in the direction of MME to SGW and SGW to PGW. The Create Session Request is used to notify the PGW of the Bearer requested by the UE and to establish a signaling tunnel between MME and SGW as well as signaling and user-plane tunnel between SGW and PGW.
12. **Create Session Response:** GTP-Cv2 operation sent in the direction of PGW to SGW and SGW to MME. The Create Session Response is used to setup the S5/S8 Bearer (SGW ↔ PGW) and a signaling tunnel between SGW and MME.
13. **EMM Attach Accept and ESM Activate Default EPS Bearer Context Request:** NAS Operation sent in the direction of MME to UE. The ESM Activate Default Bearer Request message is used to provide the UE with an IP address for the requested APN as well as the assigned QoS parameters.
14. **EMM Attach Complete and ESM Activate Default EPS Bearer Context Accept:** NAS Operation sent in the direction of UE to MME. The combined EMM and ESM message is used by the UE to acknowledge completion of the Attach Request and Default EPS Bearer establishment. A DRB is established between the UE and eNB.

14.3 Local Breakout

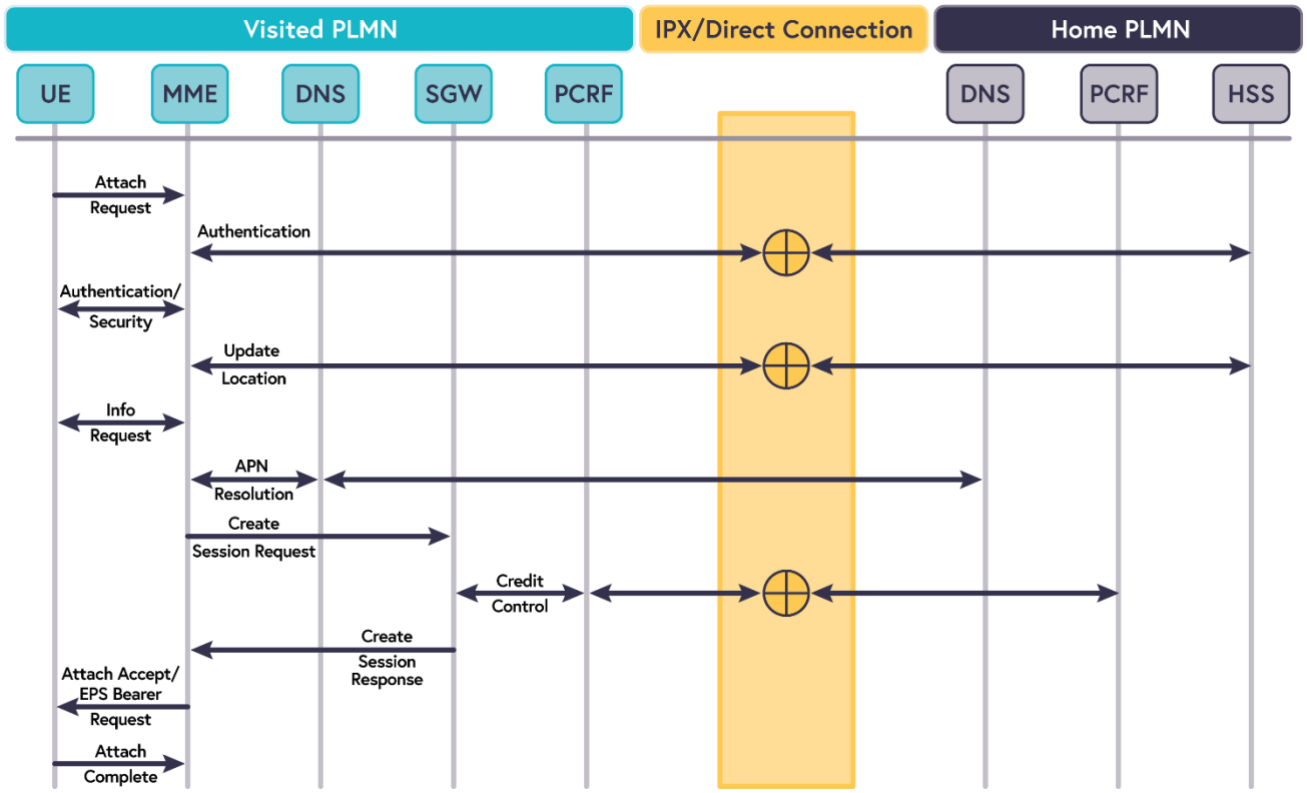

Figure 17: LTE Registration with LBO Call Flow

1. **EMM Attach Request and ESM PDN Connectivity Request:** NAS Operation sent in the direction of UE to MME (via eNB). The ESM PDN Connectivity Request message is combined with the EMM Attach Request message. The EPS Mobile Identity will be included within the message as either the IMSI or GUTI. If the GUTI is used, and not known by the MME, the MME would initiate an EMM Identity Request procedure to obtain the IMSI of the UE (not shown).
2. **Authentication Information Request/Answer (AIR/AIA):** DIAMETER operation initiated by an MME to HSS to request unique authentication vectors from the HSS.
3. **EMM Authentication Request:** NAS Operation sent in the direction of MME to UE (via eNB). The EMM Authentication Request message is used to challenge the UE with the authentication vector provided by the HSS. Authentication is mutual and the UE will ensure the network originating the Authentication Request message is valid.
4. **EMM Authentication Response:** NAS Operation sent in the direction of UE to MME (via eNB). The EMM Authentication Response message is used to provide the RES after the UE has completed processing the Authentication Request. The MME will check the RES with the XRES provided by the HSS.
5. **EMM Security Mode Command:** NAS Operation sent in the direction of MME to UE (via eNB).
6. **EMM Security Mode Complete:** NAS Operation sent in the direction of UE to MME (via eNB).

7. **ESM Information Request:** NAS Operation sent in the direction of MME to UE (via eNB). The ESM Information Request message is used to obtain the APN the UE wants to use in order to establish a Default EPS Bearer.
8. **ESM Information Response:** NAS Operation sent in the direction of UE to MME (via eNB). The ESM information Response message is used by the UE to provide the APN to be used for the Default EPS Bearer.
9. **Update Location Request/Answer (ULR/ULA):** DIAMETER operation initiated by an MME to HSS to notify HSS of a subscriber registration attempt and to request subscription data. The HSS will always return a ULA for a ULR which would include a Result Code of Diameter_Success and include the subscription data or one of the 3GPP 29.274 defined rejection codes.
10. **APN Resolution:** After an optional subscription check by an MME to ensure the requested APN is allowed by an HSS an MME will initiate a DNS procedure with the query type of NAPTR to identify the PGW Replacement names for the APN FQDN. A second A record query may be initiated if necessary to obtain the A record (IPv4 address) of the PGW replacement name.
11. **Create Session Request:** GTP-Cv2 operation sent in the direction of MME to SGW and SGW to PGW. Within the LBO model, the PGW is assumed to be collocated with the SGW. The Create Session Request is used to notify the PGW of the Bearer requested by the UE and to establish a signaling tunnel between MME and SGW as well as signaling and user-plane tunnel between SGW and PGW.
12. **Credit Control Request/Response:** Diameter operation initiated by the PCEF function of the PGW towards a PCRF. In the LBO model, the V-PCRF would forward the Credit Control Request to the H-PCRF over the S9 interface to obtain the rules for the bearer in the Credit Control Response.
13. **Create Session Response:** GTP-Cv2 operation sent in the direction of PGW to SGW and SGW to MME. The Create Session Response is used to setup the S5 Bearer (SGW ↔ PGW) and a signaling tunnel between SGW and MME.
14. **EMM Attach Accept and ESM Activate Default EPS Bearer Context Request:** NAS Operation sent in the direction of MME to UE. The ESM Activate Default Bearer Request message is used to provide the UE with an IP address for the requested APN as well as the assigned QoS parameters.
15. **EMM Attach Complete and ESM Activate Default EPS Bearer Context Accept:** NAS Operation sent in the direction of UE to MME. The combined EMM and ESM message is used by the UE to acknowledge completion of the Attach Request and Default EPS Bearer establishment. A DRB is established between the UE and eNB.

15 Wholesale Roaming Billing and Settlement

In order to provide wider coverage to its users, mobile networks must sign agreements with Service Providers and Partners. This section outlines the different agreement and billing areas to be addressed when a signing a wholesale roaming agreement. Specifically for this section, the terms in Table 4 are applicable.

Table 4: Wholesale Roaming Billing and Settlement Terms

Term	Description
Accrual Basis Accounting	Accrual basis accounting recognizes business revenue and matching expenses when they are generated—not when money changes hands.
Hub	A company that provides services to facilitate connections between Partners. A Hub may act as a Service Provider or a Partner.
Partner	Any network that may provide roaming reach for a network provider. A Hub may act as a Partner, by taking financial liability for wholesale billing and settlement for the networks connected to the Hub.
Private Interface	The relationship between a network operator and its Service Provider(s) is defined as anything that a network operator may need to do to support the Public Interface. It is the network operator responsibility to ensure that any Service Provider complies with industry standards on its behalf. These requirements are not a part of any industry documentation and must be managed by each network operator.
Public Interface	The relevant industry documentation describes the requirements to facilitate wholesale roaming billing and settlement. It is the network operator responsibility to ensure that all Public Interface requirements are supported, either internally, or by a Service Provider on its behalf.
Served Party	The Party who owns the primary relationship with the subscriber/device.
Service Provider	Any Party that provides services to facilitate connectivity between Partners. A Hub may act as a Service Provider.
Serving Party	The Party who serves the roaming subscriber/device.
Accrual Basis Accounting	Accrual basis accounting recognizes business revenue and matching expenses when they are generated—not when money changes hands.
Hub	A company that provides services to facilitate connections between Partners. A Hub may act as a Service Provider or a Partner.

15.1 Agreement

Before launching any new roaming service, the Parties must sign Agreements with Partners and Service Providers to support wholesale roaming agreements. This section provides information on the following types of Agreements to support Wholesale Roaming Billing and Settlement:

All agreements should contain Terms and Conditions, including any legal framework needed to facilitate the execution and support of the Agreement.

15.1.1 Service Provider Agreement

Service Provider Agreements are agreements with service providers to facilitate Operational and Financial exchanges with Roaming Partners. A Service Provider may act as an Authorized Receipt Point (single

connection) for management of the agreed operational and financial exchanges with a client's Partners. A Service Provider agreement supports the Private Interface.

15.1.2 Partner Agreements

Partner Agreements contain the elements needed to support Wholesale Roaming Billing and Settlement, when launching, or updating a new Agreement. As the wholesale arrangement between two Parties may be somewhat dynamic, the Agreement should be set up so that areas that require frequent update may be changed without re-signing the agreement. A Partner Agreement supports the Public Interface.

Partner Agreements may contain several annexes as defined below:

1. Common Annex: Processes/procedures and information that are common (same between the Parties) such as invoicing frequency, netting requirements, operational report exchanges, and Service Level specifics.
2. Individual Annexes: Processes/procedures and information that are not common (unique to each Party), there are currently two types of individual annexes:
    a. Operational Data – contacts for specific operational areas
    b. Charging Information – rates to be charged for roaming on each other's networks.

15.1.3 Hub Agreements

Hubs may act as Service Providers or Partners and contain the relevant combination of elements from either the Service Provider agreement, or the Partner Agreement, and any other needed information.

15.2 Interfaces

To support all wholesale roaming billing interfaces, this document uses two types of interfaces as depicted in

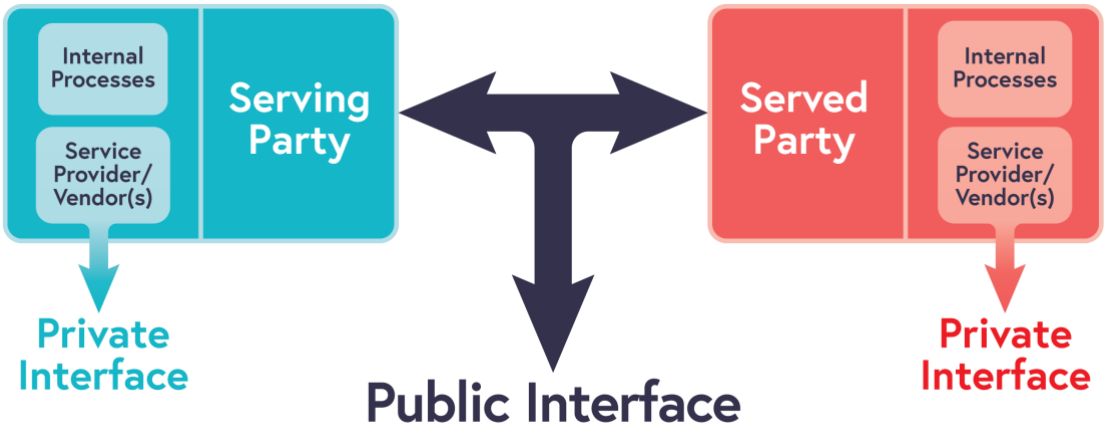

Figure 18. All industry documentation is written to support Public Interface only (Agreement between network operators). Network operators may use Service Providers to satisfy agreements however Service Providers represent network operators.

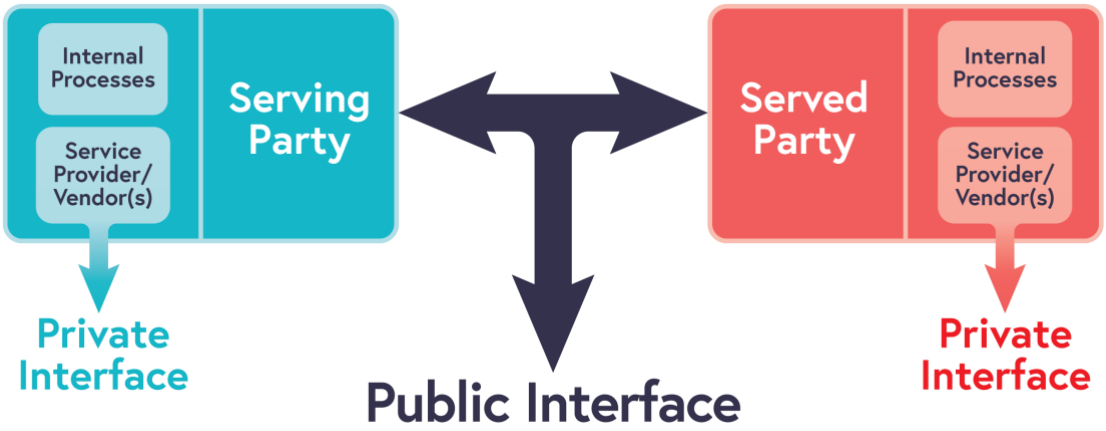

Figure 18: Private vs Public Interface

15.3 Supporting Wholesale Billing and Settlement Agreements

This section provides a high-level list of activities that are needed to support wholesale billing and settlement agreements:

- Operational Procedures - information needed to establish and facilitate billing, and other data with Partners.
- Financial Procedures – processes to support invoicing, settlement, and payment

15.3.1 Operational Procedures

This section contains Operational Procedures that must be established and maintained with Partners when launching a new agreement or supporting an existing agreement.

Wholesale roaming billing exchange should consider limiting detailed record exchange where possible. For example, if information is available to both roaming partners, detailed data exchange should be avoided.

1. Testing – Pre-Launch
    a. Exchange of devices and/or SIMs to be used for testing.
    b. Agreement of test scope – tests to be performed, and expected success criteria.
    c. Assignment of resources to facilitate testing activity completion as agreed.
2. Reconciliation and Exchange Processes
    a. Billing data exchange with Partner as needed (Note: detailed usage records should only be exchanged when necessary to support billing or reconciliation functions).
    b. Report exchange contents and frequency, to facilitate reconciliation activities as agreed during each invoicing period.
    c. Billing data exchange with Service Provider to support accrual basis accounting.
    d. Traffic reconciliation activities and dispute resolution, any pre-invoicing activities to keep disputes out of money.

3. Service Level conditions – for Service Provider:
    a. Any measurements agreed between the Parties where commitments are agreed; for example, Service availability, report delivery timeframes to Partner, etc.
    b. Associated financial penalties associated with Service Level measurements.

15.3.2 Financial Procedures

This section contains Financial Procedures that must be established and maintained with Partners when financial liability is transferred (via invoice exchange).

1. Invoice Production:
    a. Validation of invoices produced, to be sent for payment.
    b. Distribution of invoices to Partners.
    c. Management of invoice disputes (credit note applications).
2. Invoice receipt from Partners:
    a. Invoice reconciliation activities.
    b. Raising Invoice disputes (credit/debit note applications) .
3. Financial Clearing Activities:
    a. Calculation of final positions (support netting).
    b. Other calculations that require invoices to calculate (longer term commitments, etc.).
4. Service Level Conditions:
    a. Any measurements agreed between the Parties where commitments are agreed (for example Service availability, Invoice delivery timeframes, etc.).
    b. Associated financial penalties associated with Service Level measurements.

15.4 Summary

The contract structures, interface approach, and process outlines have been implemented in other technologies and is working in practice. Therefore, OnGo Alliance has the unique opportunity to learn from other industries when designing its wholesale roaming billing and settlement processes.

As stated earlier in this section, wholesale roaming billing exchange should consider limiting detailed record exchange where possible. For example, if information is available to both roaming partners, detailed data exchange should be avoided. Similar work is being done in GSM Association and Wireless Broadband Alliance (WBA) Working Groups to limit detailed record exchange to specific Local Breakout scenarios, when traffic is not available to both Parties. This process is generically called Billing and Charging Evolution (BCE) and focusses on the optimization of wholesale processes, that can be used for any roaming agreement, both with the same technology, and cross-technology.

Additional BCE specific documentation is available for GSMA members in the Wholesale Agreements and Solutions (WAS) group [40], Interoperability Data specifications and Settlement Group (IDS) [41] and the GSMA North America Wholesale Agreement & Data Interoperability WAS/IDS group [42].

16 Summary of Key Issues and Mitigation Options

Each of the potential roaming options discussed in the paper present challenges towards a successful and sustainable implementation. The intention of this paper has been to raise awareness towards the potential challenges of enabling roaming for a SHNI for each roaming architecture model and roaming direction. Future work and evaluation would be necessary to address the challenges to determine an economically viable and repeatable deployment option.

Figure 19 shows the total number of identified key issues for each roaming model while Figure 20 shows a consolidated view of the number of key issues categorized by a network element, function, or architecture design consideration irrespective of roaming model or direction. Neither chart suggests that any one issue is equal to another, some issues are inherently more or less complex than others. The following subsections provide a more detailed summary of the key issues by category, with correlation to the roaming model and direction.

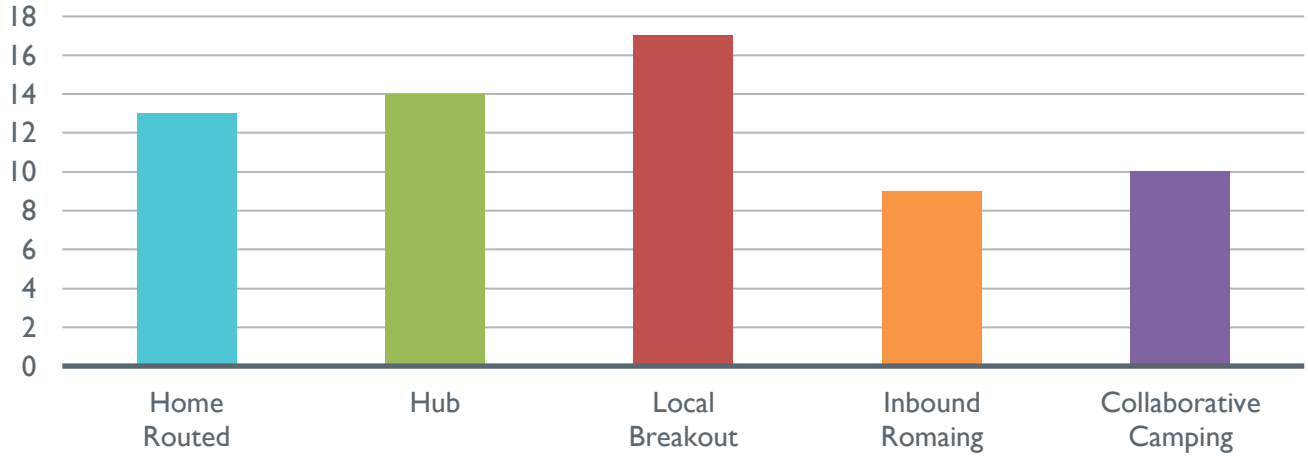

Figure 19: Key Issues by Roaming Model

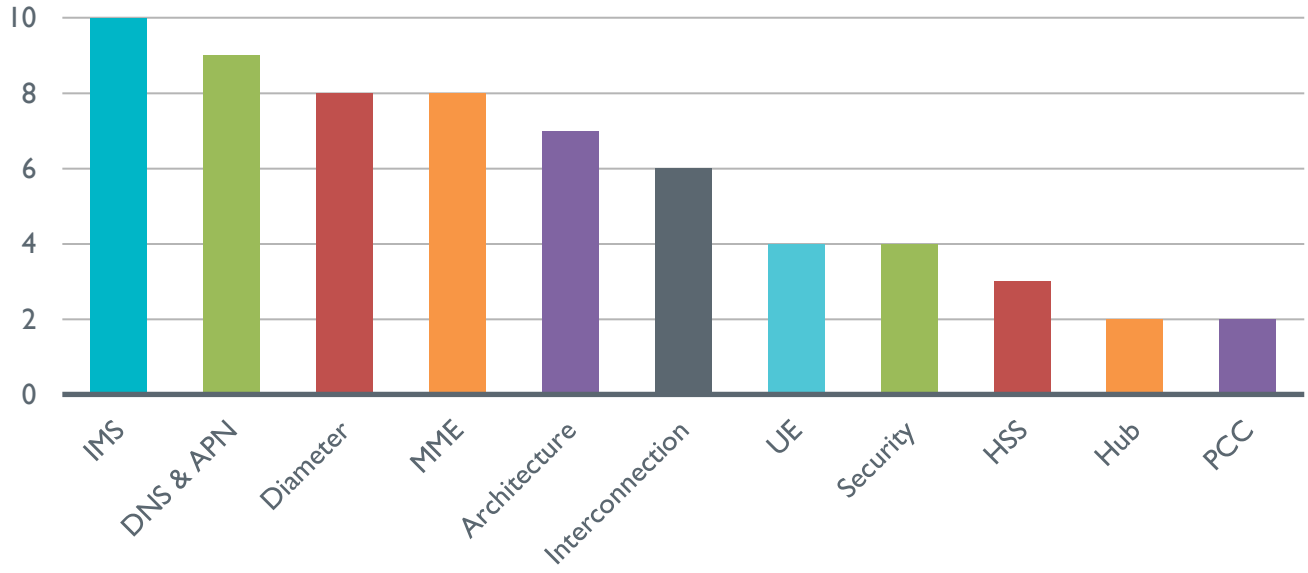

Figure 20: Key Issues by Category

16.1 IMS

IMS services represent a unique set of challenges for a private network that is using an SHNI. While at present, there appears to be minimal desire for IMS services as it relates to private network deployments, it still represents one of the most challenging aspects for all the roaming models discussed in this paper, specifically for the Private-to-Public roaming direction. As documented in sections 8 (HR), 9 (Roaming Hub) and 10 (LBO) the following are the key challenges as it relates to IMS.

16.1.1 IMS Interworking

- **LBO:** A private network offering IMS services as HR or through a Roaming Hub while leveraging LBO for other APN's would still need to maintain an S8 connection with public non-routable IP addresses as well as the IMS Core would need to interwork with LEC/LD providers.
- **LBO:** IMS services offered as LBO within the VPLMN would not work while in the Private MNO, creating an inconsistent customer experience.
- **HR:** IMS services are more susceptible to latency, jitter, and packet delay therefore, the interconnection model and bandwidth may need to be more robust than hosting other types of data applications. IMS Core would need to interwork with LEC/LD providers.
- **Hub:** IMS services are more susceptible to latency, jitter, and packet delay therefore, the interconnection model and bandwidth may need to be more robust than hosting other types of data applications. IMS Core would need to interwork with LEC/LD providers.

16.1.2 Numbering

- **LBO:** A private network offering IMS services as HR while leveraging LBO for other APN's would need to obtain telephone numbers from the appropriate numbering authority.
- **Hub:** A private network offering IMS services would need to obtain telephone numbers from the appropriate numbering authority.
- **HR:** A private network offering IMS services would need to obtain telephone numbers from the appropriate numbering authority.

16.1.3 Private network EPC

- **Hub:** S8HR IMS services require the private core must have its own IMS core.
- **HR:** S8HR IMS services require the private core must have its own IMS core.

16.1.4 APN

- **LBO:** The IMS APN is standard, therefore conflicts between a Public MNO's home and private MNO subscribers could create complex configuration in a VPLMNs IMS Core.

16.2 Diameter

Handling of Diameter signaling is critical for a 4G based deployment in any roaming direction. Diameter services are defined for use within 4G based deployments to handle signaling between a MME and HSS using the S6a interface, covering the exchange of authentication vectors and subscription data as well as many other

command codes. Regardless of the command codes, interface or roaming direction, the key issues focus on subscriber and destination realm identification. There are impacts for Diameter signaling in each of the roaming directions discussed in this paper, notably in sections 8 (HR), 9 (Roaming Hub), 10 (LBO), 11 (Private-to-Private Roaming), and 12 (Inbound Roaming).

16.2.1 Private-to-Public

- **HR:** There is no SHNI indicator in the destination realm for Diameter routing.
- **HR:** User-Name AVP routing is non-standard.
- **Hub:** User-Name AVP based routing is required.
- **LBO:** There is no SHNI indicator in the destination realm for Diameter routing.
- **LBO:** User-Name AVP routing is non-standard.

16.2.2 Public-to-Private

- **Inbound Roaming:** The private MNO would need a customized origin-realm for Diameter routing as well as maintain an SCTP association either to an IPX DEA or directly to a public MNO DEA.
- **Inbound Roaming:** Required to maintain diameter route rules for the customized origin-realm of the private MNO(s) for Diameter routing.

16.2.3 Private-to-Private

- **Collaborative Camping:** Diameter routing is symmetric, implying that a hierarchical HSS capability would mean that the first HSS in the path would insert its host name as in the Route-Record AVP and would therefore also need to process an Answer message, thus increasing load for handling of Diameter messages.

16.3 MME

The MME represents a critical network element in the EPC for handling home or roaming services. For SHNI roaming, there are issues to address in nearly all roaming models except for a Roaming Hub. The reason there are no challenges for MME handling within the Roaming Hub model for a SHNI is because the public MNO in this model is treating the SHNI as a dedicated MCC/MNC (315/010) and therefore shifts responsibility of handling the SHNI+IBN to the Roaming Hub provider. However, it should be noted there is a Diameter impact for the Roaming Hub provider as noted in the section 9 and 16.2. The following are the key issues for sections 8 (HR), 10 (LBO), 11 (Private-to-Private Roaming), and 12 (Inbound Roaming).

16.3.1 Private-to-Public

- **HR:** MME permissions may not be configurable beyond 5 or 6 digits to incorporate the SHNI MCC/MNC+IBN combination.
- **LBO:** Configuring LBO at an entire MCC/MNC level for a SHNI prevents other models from being leveraged.
- **LBO:** MME permissions may not be configurable beyond 5 or 6 digits to incorporate the SHNI MCC/MNC+IBN combination.
- **LBO:** The VPLMN-Dynamic-Address-Allowed AVP must be supported by the MME.

16.3.2 Public-to-Private

- **Inbound Roaming:** MME permissions would include the common 5- or 6-digit public MNO IMSI Number Series.

16.3.3 Private-to-Private

- **Collaborative Camping:** Configuring LBO at an entire MCC/MNC level for a SHNI prevents other models from being leveraged.
- **Collaborative Camping:** MME permissions may not be configurable beyond 5 or 6 digits to incorporate the SHNI MCC/MNC+IBN combination.
- **Collaborative Camping:** The VPLMN-Dynamic-Address-Allowed AVP must be supported by the MME.

16.4 DNS and APN

During network registration with a 4G network, or for subsequent data bearer creation the APN resolution process is critical to providing data services. For all roaming directions and models discussed in this paper there are issues to address with respect to handling APN resolution. It should be noted that there is some overlap with MME issues in terms of handling APN resolution for a SHNI, specifically that the APN-OI Replacement AVP that can be contained in a Diameter Update Location Answer is considered as an optional feature and may not be universally supported. The following issues relate to the sections 8 (HR), 9 (Roaming Hub), 10 (LBO), 11 (Private-to-Private Roaming), and 12 (Inbound Roaming).

16.4.1 Private-to-Public

- **HR:** APN-OI Replacement may not be universally supported in public MNO MMEs.
- **HR:** The APN FQDN does not contain any subscriber specific indication unless a label is included by a private MNO, in which there is no regulatory body to prevent duplication.
- **HR:** Root DNS records for a SHNI APN-OI would need to point to a common entity as the SOA record.
- **Hub:** Authoritative NS must be registered with GSMA Root DNS.
- **Hub:** DNS zone transfers or similar solution may be required if Hub redirects data bearer creation directly to private MNO PGW.
- **Hub:** APN-OI Replacement may not be universally supported in public MNO MMEs.
- **LBO:** APN-NIs for a private MNO must be configured within the home authoritative DNS and PGW and cannot overlap with any of the VPLMN home customers.

16.4.2 Private-to-Private

- **Collaborative Camping:** APN-NIs for a private MNO must be configured within the home authoritative DNS and PGW and cannot overlap with any of the VPLMN home customers.

16.4.3 Public-to-Private

- **Inbound Roaming:** Locally manage zone files for the public MNO APN-OI to authoritative hostname or leverage the IPX root DNS lookup procedure.

16.5 Architecture

Each roaming model discussed in this paper has architecture related issues that primarily focusing on whether the private network implementation can support the common roaming interfaces. As alluded to in prior sections it should not be assumed that the roaming interfaces are universally supported in a private network EPC. Therefore, there is significant similarity of the key issues covered in sections 8 (HR), 9 (Roaming Hub), 10 (LBO), 11 (Private-to-Private Roaming), and 12 (Inbound Roaming) related to support for the roaming interfaces.

16.5.1 Private-to-Public

- **HR:** Roaming interfaces for S6a and S8 must be supported in the Private EPC.
- **Hub:** Roaming interfaces for S6a and S8 may be required in the private MNO for hybrid models
- **LBO:** Roaming interfaces for S6a and S9 must be supported in the Private EPC.
- **LBO:** LBO usage globally is unpopular and is considered as obsolete by GSMA.

16.5.2 Private-to-Private

- **Collaborative Camping:** LBO usage globally is unpopular and is considered as obsolete by GSMA.
- **Collaborative Camping:** Roaming interfaces for S6a must be supported in the Private EPC.

16.5.3 Public-to-Private

- **Inbound Roaming:** Roaming interfaces for S6a and S8 must be supported in the Private EPC.

16.6 Interconnection

The most common and scalable method of interconnecting between MNOs is through one or more IPX providers to create global reachability. While there is possibility for the interconnection to be direct, this could present economic and technical challenges for implementing and maintaining multiple direct connections. Irrespective of a direct vs IPX interconnection strategy, there are key issues to account for in all roaming models and directions as discussed in sections 8 (HR), 9 (Roaming Hub), 10 (LBO), 11 (Private-to-Private Roaming), and 12 (Inbound Roaming).

16.6.1 Public-to-Private

- **HR:** The private MNO must use Public, non-Internet routable IPv4 addresses as well as a unique ASN for BGP peering and interconnection.
- **Hub:** The Roaming Hub provider must use Public, non-Internet routable IPv4 addresses as well as a unique ASN for BGP peering and interconnection.
- **Hub:** The Hub provider must inter-connect to public MNOs via IPX.
- **LBO:** The private MNO must interconnect directly or through an IPX for Diameter SCTP based connections.

16.6.2 Private-to-Public

- **Inbound Roaming:** The private MNO must use Public, non-Internet routable IPv4 addresses as well as a unique ASN for BGP peering and interconnection.

16.6.3 Private-to-Private

- **Collaborative Camping:** The private MNOs must interconnect directly or through an IPX for Diameter SCTP based connections.

16.7 Security

Securing network traffic between connected MNOs is a critical aspect regardless of the roaming direction or model. While the specific firewall configurations may differ for each roaming model the premise is still the same. Initial configuration, management, and ongoing sustainment of firewall permissions to secure a private network that interconnects in any manner to another network is required.

- **HR:** The private MNO would need to configure and maintain firewall rules for the connected Public MNO(s) backbone IP ranges and associated ports for DNS, Diameter and GTP traffic.
- **Hub:** The private MNO and/or Roaming Hub provider would need to configure and maintain firewall rules for the connected Public MNO(s) backbone IP ranges and associated ports for DNS, Diameter and GTP traffic.
- **LBO:** The private MNO would need to configure and maintain firewall rules for the connected Public MNO(s) backbone IP ranges and associated ports for Diameter.
- **Inbound Roaming:** The private MNO would need to configure and maintain firewall rules for the connected Public MNO(s) backbone IP ranges and associated ports for DNS, Diameter and GTP traffic.

16.8 End User Devices

Device compatibility is a broad topic range and shows potential challenges in 3 of the roaming models. The primary impact for EUDs as documented in sections 8 (HR), 9 (Roaming Hub) and 10 (LBO) relates to IMS capabilities although there is also potential impact for section 12 (Inbound Roaming) as well. Section 6 also notes that to use a EUD in a commercial network, i.e., in the Private-to-Public direction, the EUD would need to support the licensed spectrum bands of that commercial operator. That is potentially a minimal challenge as most EUDs are already supportive of many global licensed bands. Regarding frequency band support, it is more likely that EUD challenges would impact the CBRS band for use inside the SHNI private network.

- HR: For IMS to be supported, the private MNO UE could need a custom SHNI+IBN SIP client.
- Roaming Hub: For IMS to be supported, the private MNO UE could need a custom SHNI or SHNI+IBN SIP client.
- LBO: For IMS to be supported, the private MNO UE could need a custom SHNI or SHNI+IBN SIP client.
- Inbound Roaming: A UE that is connected to its HPLMN broadcast will remain camped on the HPLMN even when in range of the private MNO broadcast.

16.9 HSS

The HSS performs critical functions related to authentication and management of subscription data transfer to an MME during 4G network registration. Without the ability to reach the correct HSS for the SHNI end user to retrieve the correct authentication vectors and subscription data network registrations will be unsuccessful. Many of the key issues related to the retrieval of this critical elements have already been summarized related to Diameter and MME sections, so the following detail from sections 10 (LBO), 11 (Private-to-Private Roaming), and 12 (Inbound Roaming) is intended to be specific to the HSS with the presumption that Diameter routing challenges have already addressed.

- **LBO:** The VPLMN-Dynamic-Address-Allowed AVP must be supported by the HSS.
- **Inbound Roaming:** The public MNO would be unable to differentiate the VPLMN ID of the private MNO when each is using the SHNI for network broadcast.
- **Collaborative Camping:** Commonly, an HSS is single network element, and a hierarchical structure implies an HSS includes Diameter proxy capabilities which would more commonly exist as a Diameter function prior to signaling reaching an HSS.

16.10 Roaming Hub

The Roaming Hub architecture model specifically relates to the Private-to-Public roaming direction and while there are many key issues for this model as discussed in section 9 (Roaming Hub), most have been summarized already within this section. The following key issues focus more on business decisions and best practices for leveraging a roaming hub model to provide Private-to-Public roaming capabilities.

- **Hub:** A single provider should host the hub function for the entire SHNI.
- **Hub:** The Hub provider must establish and launch roaming agreements for the SHNI.

16.11 Policy and Charging Control

The PCC component of an EPS is critical for providing the rules related to a data bearer. The premise of the PCC related issues captured in the sections 10 (LBO) and 11 (Private-to-Private Roaming) has been on handling of QoS rules. Additional challenges may exist for online or offline charging systems, but those nuances are outside the scope of this paper.

- **LBO:** QoS rules and policy must be negotiated and possibly configured in a custom manner for each SHNI.
- **Collaborative Camping:** QoS rules and policy must be negotiated and possibly configured in a custom manner for each SHNI.

17 5G SA Roaming

Within the private network 5G SA can be utilized alongside a 4G EPC for CBRS SHNI deployments. However, the global telecommunications industry will need more time to evolve 5G SA Roaming commercially, therefore, this is a forward-looking topic that will require extensive investigation, assessment, and commercial MNO readiness before it could be realized for a private network. At the time this paper was created, thirty-four operators globally have launched 5G SA cores. Within the United States where OnGo is focused only two operators have launched 5G SA cores.

Currently, several operators are testing with partners to validate 5G SA roaming call flows and prepare for commercial launches. 5G SA roaming is gaining traction across the mobile space, thus. However, even with a few announcements of successful 5G SA roaming connections by the beginning of 2023, to obtain the full scope and promise of 5G SA roaming, operators will need to develop or obtain the required support systems and the Value-Added Services (VAS) that operators depend on today for 3G and 4G roaming. Aside from the immediate technical requirements of security and the new 5G core functions, operators must consider the monitoring and analytics, transaction clearing, commercial roaming negotiations and testing for roaming role out. Starting with traditional roaming concepts, the roaming environment will change and implement more local/regional breakout use cases which will bring content closer to the user vs. the historical default to home routing everything. Other use cases such as network slicing mobility will drive the need for more collaboration between mobile operators.

GSMA together with 3GPP are working on extending definitions to complement the initial 3GPP 5G SA roaming architecture to include also roaming HUBs and Roaming VAS. As an example, from a standards perspective, the GSMA 5GMRR (5G Mobile Roaming Revisited) taskforce will provide industry guidelines on the 5G roaming models to be supported within the operator ecosystem [43].

Beyond commercial MNO and industry readiness, more clarity is also needed on the benefit and use cases related to CBRS SHNI users in a 5G SA roaming environment. For these reasons, 5G SA roaming was considered as out of scope for this paper and further work would be necessary to adequately provide identification of key issues and challenges.

18 References

[1] "About Us," GSM Association, . [Online]. Available: https://www.gsma.com/aboutus. [Accessed].

[2] "History," GSM Association, [Online]. Available: https://www.gsma.com/aboutus/history.

[3] "Membership Types," GSM Association, [Online]. Available: ttps://www.gsma.com/membership/membership-types/.

[4] "About 3GPP," 3GPP, [Online]. Available: https://www.3gpp.org/about-3gpp.

[5] "Membership," 3GPP, [Online]. Available: https://www.3gpp.org/about-3gpp/membership.

[6] "3GPP Membership Query Form," 3GPP, [Online]. Available: https://webapp.etsi.org/3gppmembership/QueryForm.asp.

[7] GSM Association, "BA.46 Non-Terrestrial Roaming Principles version 6.3," [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads/2012/06/BA4663.pdf.

[8] GSM Association, "IR.21 GSM Association Roaming Database, Structure and Updating Procedures version 9.1," [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads/2013/07/IR.21-v9.1.pdf.

[9] GSM Association, "IR.88 EPS Roaming Guidelines v25.0," [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads/IR.88-v25.0-17.pdf.

[10] GSM Association, "NG.113 5GS Roaming Guidelines version 4.0," [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//NG.113-v4.0.pdf.

[11] 3GPP, "3GPP Specification Status Report," 3GPP, [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm.

[12] 3GPP, "3GPP TS 23.501, System Architecture for the 5G System, Release 17," [Online]. Available: http://www.3gpp.org/.

[13] GSM Association, "R.34 Guidelines for IPX Provider networks (Previously InterService Provider IP Backbone Guidelines) v17.0," [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//IR.34-v17.0-3.pdf.

[14] GSM Association, "IR.40 Guidelines for IPv4 Addressing and AS Numbering for GPRS Network Infrastructure and Mobile Terminal v8.0," [Online]. Available: https://www.gsma.com/newsroom/resources/ir-40-guidelines-for-ipv4-addressing-and-as-numbering-for-gprs-network-infrastructure-and-mobile-terminal-v8-0/attachment/ir-40-v8-0/.

[15] GSM Association, "AA.80 IP Packet eXchange Service Agreement, version 3.2," [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2012/03/aa8032.pdf.

[16] IETF, "IETF RFC 3246, An Expedited Forwarding PHB (Per-Hop Behavior)," [Online]. Available: https://www.rfc-editor.org/rfc/rfc3246.

[17] 3GPP, "3GPP TS 23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access; Release 17," [Online]. Available: http://www.3gpp.org/.

[18] GSM Association, "IR.80 Technical Architecture Alternatives for Open Connectivity Roaming Hubbing Model version 3.0," [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//IR.80-v3.0-3.pdf.

[19] OnGo Alliance, "OnGo Alliance," [Online]. Available: https://ongoalliance.org.

[20] OnGo Alliance, "OnGo Certified Devices," [Online]. Available: https://ongoalliance.org/certification/ongo-certified-devices/.

[21] D. Kim, "Non-Public Networks (NPN)," 15 12 2022. [Online]. Available: https://www.3gpp.org/technologies/npn.

[22] OnGo Alliance, "OnGo Identifiers Flyer - OnGo Alliance," [Online]. Available: https://ongoalliance.org/resource/ongo-identifiers-flyer/.

[23] GSM Association, "IR.77 InterOperator IP Backbone Security Req. For Service and Inter operator IP backbone Providers, v5.0," [Online]. Available: https://www.gsma.com/security/resources/ir-77-interoperator-ip-backbone-security-req-for-service-and-inter-operator-ip-backbone-providers-v5-0/.

References

[24] OnGo Alliance, "OnGo Private LTE Deployment Guide," [Online]. Available: https://ongoalliance.org/resource/ongo-private-lte-deployment-guide/.

[25] OnGo Alliance, "OnGo Neutral Host Network Deployment Guide," [Online]. Available: https://ongoalliance.org/resource/ongo-nhn-deployment-guide/.

[26] 3GPP, "3GPP TS 24.301, Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3; Release 15," [Online]. Available: http://www.3gpp.org/.

[27] IETF, "IETF RFC 6733, Diameter Base Protocol," [Online]. Available: https://www.rfc-editor.org/rfc/rfc6733.html.

[28] 3GPP, "3GPP TS 29.272, Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol, Release 16," [Online]. Available: http://www.3gpp.org/.

[29] 3GPP, "3GPP TS 23.003, Numbering, Addressing and Identification, Release 16," [Online]. Available: http://www.3gpp.org/.

[30] OnGo Alliance, "ONGO-TS-1002, CBRS Network Services Stage 2 and 3 Specification, v4.1.0," [Online]. Available: https://ongoalliance.org/resource/network-services-stage-2-and-3-technical-specifications/.

[31] 3GPP, "3GPP TS 29.303, Domain Name System Procedures; Stage 3; Release 16," [Online]. Available: http://www.3gpp.org/.

[32] GSM Association, "IR.92 IMS Profile for Voice and SMS, Version 15.0," [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads/IR.92-v15.0-4.pdf.

[33] 3GPP, "3GPP TS 23.203, Policy and Charging Control Architecture, Release 16," [Online]. Available: http://www.3gpp.org/.

[34] W. Cutler, "Your guide to accelerating VoLTE Roaming, and its importance to your business," [Online]. Available: https://www.gsma.com/services/blog/guide-accelerating-volte-roaming/.

[35] 3GPP, "3GPP TS 29.215, Policy and Charging Control (PCC) Over S9 Reference point; Stage 3, Release 16.," [Online]. Available: http://www.3gpp.org/.

[36] 3GPP, "3GPP TS 29.212, Policy and Charging Control (PCC); Reference Points, Release 16.," [Online]. Available: http://www.3gpp.org.

[37] OnGo Alliance, "ONGO-TS-1004, CBRS Network Services – Private CBRS / Non-Public Network Geofencing, Policies, and TAC Collision Avoidance, v5.1.0," [Online]. Available: https://ongoalliance.org/wp-content/uploads/2022/07/OnGo-TS-1004-V5.0.0_Published-December-15-2022.pdf.

[38] OnGo Alliance, "CBRSA-TR-1003, Feasibility Study of CBRS RAN Sharing (CBRS MOCN) for Neutral Hosting," [Online]. Available: https://workspace.ongoalliance.org/wg/OnGo/document/1282.

[39] 3GPP, "3GPP TS 23.251, Network sharing; Architecture and functional description, Release 16.," [Online]. Available: http://www.3gpp.org/.

[40] GSM Association, "Wholesale Agreements and Solutions Group," [Online]. Available: https://www.gsma.com/aboutus/workinggroups/wholesale-agreements-and-solutions-group.

[41] GSM Association, "Interoperability Data specifications and Settlement Group," [Online]. Available: https://www.gsma.com/aboutus/workinggroups/interoperability-data-specifications-and-settlement-group.

[42] GSM Association, "Wholesale Agreement & Data Interoperability," [Online]. Available: https://www.gsma.com/northamerica/was-ids/.

[43] GSM Association, "NG.132 Report 5G Mobile Roaming Revisited (5GMRR) Phase 1, v2.0," [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//NG.132-v2.0-1.pdf.

19 Definitions & Abbreviations

19.1 Definitions

Term	Definition
4G	A fourth-generation wireless communications technology. For mobile cellular networks, this generally refers to the 3GPP's LTE technology, though LTE didn't meet the fourth-generation requirements until the release of LTE Advanced (LTE-A)
5G Core (5GC)	The core network component of the 5GS, as defined by the 3GPP.
5G New Radio (5G NR)	The air interface of the 5GS. In common parlance, NR is often used to refer to the entire 5GS.
5G System (5GS)	The complete fifth generation wireless communications technology as defined by the 3GPP. Includes the air interface (5G NR) and the core network (5GC).
Core Network (CN)	The component of a wireless network responsible coordinating elements of the network, and providing the essential services needed to make the network function – such as authentication, traffic routing and mobility management, billing, interfacing with other networks, etc.
EPS-AKA	Evolved Packet system and Key Agreement protocol. A security mechanism that is (more or less) hard-wired to the system. It allows for secure negotiation for encryption algorithms during a session, as well as allowing upgrades or deprecation of cryptographic algorithms only.
EPS	Evolved Packet System. Commonly referred to as 4G. It is comprised of the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the IP-based Evolved Packet Core (EPC).
eNodeB	Evolved Node B – A 4G LTE base station
Fixed Wireless Access (FWA)	Providing broadband connectivity wirelessly to non-mobile devices.
gNodeB	Next Generation Node B – a 5G NR base station
Long Term Evolution (LTE)	The 3GPP's 4th generation wireless cellular communication standard. Technically only refers to the just the air-interface, but is commonly used to refer to the entire LTE system – the air interface, the mobile devices, and the core network.
Neutral Host Network (NHN)	A network that offers seamless service to subscribers of multiple different public networks.
OSI Model	Open Systems Interconnect Model, the standard 7-layers model of network communications
Private Cellular Network (PCN)	A network using cellular technologies to provide services to a limited set of users, and not members of the general public
User Equipment (UE)	The mobile device in a 3GPP LTE or 5G NR network. In CBRS parlance, it is an End User Device (EUD).

19.2 Abbreviations

Term	Definition
3GPP	3rd Generation Partnership Project

Definitions and Abbreviations

Term	Definition
5G	5th Generation
5G SA	5G Standalone
5GC	5G Core
5GMRR	5G Mobile Roaming Revisited
5GS	5G System
ACL	Access Control List
AIA	Authentication Information Answer
AIR	Authentication Information Request
APN	Access Point Name
APN-NI	APN Network Identifier
APN-OI	APN Operator Identifier
ARIB	Association of Radio Industries and Businesses
AS	Autonomous System
ASN	Autonomous System Number
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
AVP	Attribute Value Pair
BCE	Billing and Charging Evolution
BGP	Border Gateway Protocol
CBRS	Citizens Broadband Radio Service
CBRS NID	CBRS Network Identifier
CBRS SHNI	CBRS Shared Home Network Identifier
CBSD	CBRS Device
CCA	Credit Control Answer
CCR	Credit Control Request
CCSA	China Communications Standards Association
CDMA	Code Division Multiple Access
CEPT	Confederation of European Posts and Telecommunications
CoS	Class-of-Service
CP	Control Plane
CSR	Create Session Request
CT	Core Network & Terminals
DA	Diameter Agent
DEA	Diameter Edge Agent
DNS	Domain Name System
DRB	Data Radio Bearer
DSCP	Differentiated Services Field Codepoints
EMM	EPS Mobility Management
eNB	eNodeB
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESM	EPS Session Management
ETSI	European Telecommunications Standards Institute
EUD	End User Device

Definitions and Abbreviations

Term	Definition
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FCC	Federal Communications Commission
FQDN	Fully Qualified Domain Name
FR	Frame Relay
GAA	General Authorized Access
GHz	Gigahertz
gNB	gNodeB
GPRS	General Packet Radio Service
GRX	GPRS Roaming eXchange
GSM	Global System for Mobile Communications
GSMA	GSM Association
GTP	GPRS Tunnelling Protocol
GTP-U	GTP-User plane
GTP-Cv2	GTP Control Plane version 2
GUTI	Globally Unique Temporary ID
H-PCRF	Home PCRF
HPLMN	Home PLMN
HR	Home Routed
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HTTP2	HyperText Transfer Protocol 2
IBN	IMSI Block Number
iDEN	Integrated Digital Enhanced Network
IDR	Insert-Subscriber Data Request
IDS	Interoperability Data specifications and Settlement Group
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPsec	IP Security
IPX	IP eXchange
ITU	International Telecommunications Union
IX	Internet exchange
KPI	Key Performance Indicator
LBO	Local Breakout
LD	Long Distance
LEC	Local Exchange Carrier
LTE	Long Term Evolution
MCC	Mobile Country Code
MHz	Megahertz
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Centre
MNC	Mobile Network Code

Definitions and Abbreviations

Term	Definition
MNO	Mobile Network Operator
MOCN	Multi-Operator Core Network
MORAN	Multiple Operator Radio Access Network
MSIN	Mobile Subscriber Identity Number
MVNO	Mobile Virtual Network Operator
mW	Milliwatt
NANPA	North American Numbering Plan Association
NAPTR	Naming Authority Pointer
NAS	Non-Access-Stratum
NG	Next Generation
NHN	Neutral Host Network
Non-GBR	Non-guaranteed bitrate
NR	New Radio
NS	Nameserver
OTT	Over-The-Top
PAL	Priority Access License
PCC	Policy and Charging Control
PCEF	Policy and Control Enforcement Function
PCF	Policy Control Function
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PGW	Packet Data Network Gateway
PLMN	Public Land Mobile Network
PLMN ID	PLMN Identifier
PRD	Permanent Reference Document
PSP	Participating Service Provider
QCI	QoS Class Identifier
QoS	Quality-of-Service
RAEX	Roaming Agreement Exchange
RAN	Radio Access Network
REST	Representational State Transfer
RTP	Real-Time Transport Protocol
S1-U	S1 User plane
S8HR	S8 Home Routed
SAS	Spectrum Access System
SCTP	Stream Control Transmission Protocol
SEPP	Security Edge Protection Proxy
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SHNI	Shared Home Network Identifier
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Assurance/Agreements
SMS	Short Message Service

Term	Definition
S-NAPTR	straightforward-NAPTR
SOA	Start of Authority
SS7	Signaling System Number 7
TAU	Tracking Area Update
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TEID	Tunnel Endpoint ID
TOS	Type of Service
TSDSI	Telecommunications Standards Development Society, India
TSG	Technical Specification Groups
TTA	Telecommunications Technology Association
TTC	Telecommunication Technology Committee
UDP	User Datagram Protocol
UE	User Equipment
ULA	Update Location Answer
ULR	Update Location Request
UMTS	Universal Mobile Telecommunications System
UP	User Plane
UPF	User Plane Function
VAS	Value-Added Services
ViLTE	Video over LTE
VoIP	Voice over IP
VoLTE	Voice over LTE
VoWiFi	Voice over Wi-Fi
V-PCRF	Visited PCRF
VPLMN	Visited PLMN
VPN	Virtual Private Network
WAS	Wholesale Agreements and Solutions
WBA	Wireless Broadband Alliance
WCDMA	Wideband Code Division Multiple Access